IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Minutes Mixed Mode Plenary **Session 12-17 Mar 2023** |
| Date: 2023-03-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | Sky Group/Comcast | Brussels, Belgium |  | amelia.ieee@andersdotter.cc |

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 12-17 March 2023. The on-site location for the meeting was Atlanta, Georgia, USA. "Local time" refers to local time in Atlanta, Georgia, 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 13 March 2023, 13:30 local time.**

Chair calls meeting to order at 13:37 local time.

Agenda slide deck: [11-23-0189r3](https://mentor.ieee.org/802.11/dcn/23/11-23-0189-03-00bi-march-plenary-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 11-23-0189r3 (slide #18)**
	1. Further submissions added to the agenda.
	2. Agenda as amended approved by unanimous consent (30 remote participants, 15 in-room)
5. **Administration**
	1. **Motion #29:** Approve the minutes for:

	2023 January 802.11 Electronic Interim: [11-23/0206r1](https://mentor.ieee.org/802.11/dcn/23/11-23-0206-01-00bi-january-interim-session-minutes-tgbi.docx),

TGbi Teleconferences: [11-23/0228r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0228-00-00bi-tgbi-teleconference-minutes-16-february-2023.docx) (16 Feb), [11-23/0278r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0278-00-00bi-tgbi-teleconference-minutes-2-march-2023.docx) (2 Mar)

Moved: Jerome Henry

Seconded: Stephen Orr

Approved by unanimous consent (30 remote participants, 15 in-room)

* 1. Discussion on teleconferences, meeting slots this week.
1. **Technical Presentations**
	1. **OTA MAC Address Change (**[**11-23/0268r0**](https://mentor.ieee.org/802.11/dcn/23/11-23-0268-00-00bi-ota-mac-address-change.pptx))**,** Carol Ansley (Cox)

	Jerome Henry chairs the meeting while Carol Ansley is presenting.

	Proposal is to randomize SA and DA separately, by using a two new bits that indicate to surrounding STAs whether randomization after association is possible.

	**Discussion:**

	**Q:** With SA you mean the value in the TA field in the MPDU? So changing address 2?
	**A:** Yes.
	**Q:** When an association is initiated, the SA and DA addresses are the same, and only after the first MAC address change do we see a split?
	**A:** Yes.
	**C:** The RA and TA are usually involved in key generation, so if these fields are being changed that may have implications on security to consider.
	**Q:** How will we process acks in this process?
	**A:** There are timing attacks that can defeat this additional protection, but with a large amount of traffic this type of attack will be more costly to perform.
	**C:** SA and DA are tied to the DS so they have to be the same, I think. We will have to clarify the terminology here.
	**C:** If the addresses are split in this way, it will imply double calculations because you're generating two MAC addresses instead of one. That will imply some energy problems.
	**Q:** Is the benefit of this system that you avoid changes in the MAC?
	**A:** The proposal is to reduce the amount of calculations and transmissions needed.
	**C:** All the MAC addresses OTA are exposed to attackers. We should pay attention to that. We could address the A1, .., A4, (A5, A6 for mesh although they are encrypted) and see if they need additional protection.
	**Q:** Would we have different AIDs for uplink and downlink too? Or groupcast addresses?
	**A:** The basic idea is as presented, we can discuss other ramifications.
	**C:** I would not want to use PMK in the way proposed for the generation of MAC.
	**C:** It will not be sufficient with one counter in the beacon frame, if we are using that to manage the PMK for each of the stations.
	**C:** Privacy is a capability level. An AP could want to use this to choose who associates, to protect other privacy capable devices in the BSS.
	**Q:** Have you considered using an action frame rather than a beacon frame?
	**A:** A beacon frame makes sure everyone can receive the frame. An action frame has repercussions for non-AP STA that are asleep when the frame is transmitted. It also has overhead implications.

	Chair closes the queue.
	2. **MLD OTA MAC Address Change (**[**11-23/0328**](https://mentor.ieee.org/802.11/dcn/23/11-23-0328-00-00bi-mld-ota-mac-address-change.pptx)**),** Carol Ansley (Cox)

Jerome Henry chairs the meeting while Carol Ansley is presenting.

Proposal discusses implications of correlation attacks are enabled through the SN and PN at the upper MAC level. A randomized SN sequence could be pre-generated so that intercepted SN are not as easily placed.

**Discussion:**

**Q:** Our AEAD schemes depend on SN/PN not repeating. What is the probability that changing SN/PN will cause either of them to fall in a previously used range?
**Q:** Would non-sequential SN bring problems with BlockAcks?
**Q:** Your SN already needs to be changed when you change your MAC address, but if you keep the address over two transmitted frames you also keep the SN.
**A:** Some of these ideas break existing implementations. However, the SNs could not be repeated, that's a criterion.
**C:** Currently we do BlockAck scoreboarding to see which one is missing, which one is received, etc. and this relies on the SN. Changing the SN in this way would really have an impact on that.
**C:** This seems not only a problem for MLD, but also generally.

1. **AoB**Carol Ansley chairs the meeting again.No other business raised.
2. **Recess 15:27 local time.**

**2nd slot. Tuesday 17 March 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 bh.
	**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 March 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 March 2023 13:00 local time.**

1. **Chair calls the meeting to order at 13:34 local time.**
2. **Reminder of policies and procedures (see para 1-3 above under 1st slot, or para 10, 16).**
3. **Review of the agenda** [**11-23-0189r6**](https://mentor.ieee.org/802.11/dcn/23/11-23-0189-06-00bi-march-plenary-agenda.pptx) **(slide #18)**
	1. Agenda approved by unanimous consent (18 participants online, 14 on-site)
4. **Technical presentations**
	1. **A1 filtering for rotating MAC addresses** ([11-23-0414r1](https://mentor.ieee.org/802.11/dcn/23/11-23-0414-01-00bi-a1-filtering-for-rotating-mac-addresses.pptx)), Antonio de la Oliva (Interdigital, UC3M)

	Continued from para. 18.3 above.

	Proposal was updated to clarify how the active MAC address sets would impact what is visible over the air when transmitting from STA A to STA B (or vice-versa).

	**Discussion:

	Q:** Why do we still need the aaMAC address after we have the otaMAC address?
	**A:** The aaMAC address is kept because the frame is reidentified with the aaMAC after it is received. The otaMAC address is only visible over-the-air but is not used for any processing of the frame on either of the involved STA.
	**Q:** Will the aaMAC address ever bed used for transmission after the MAC address set is formed?
	**A:** If you want to include it in the MAC address set you can.
	**C:** There are some places in the standard where the A1 and A3 address are cross-referenced with each other. TDLS set-up, mesh and BSS Color are three features where we will need to check the exact sequence transactions.
	**Q:** In the set of addresses available for over-the-air transmissions, would one of those addresses be chosen randomly and if so by which mechanism?
	**A:** The MAC address set contains a set of addresses that can be generated in the way chosen by the STA.
	**C:** The size of the set could be discussed.

	**Strawpoll:** Do you agree on a solution where a set of addresses is used per STA to receive and transmit frames in order to improve their privacy?

	Yes: 4
	No: 9
	Abstain: 3
	Need more information: 9

	*Procedural note: the audio set-up between the bridge and the room is not working. Online participants restricted to text-based communication for interactions with onsite participants.*
	2. **PMKID Protection** ([11-23-0467r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0467-00-00bi-pmkid-protection.pptx)), Okan Mutgan (Nokia)

	Proposal is to allow for the simple re-location of a PMKID by introducing a key index. In large (typically non-residential) networks this will facilitate re-location of an already established PMKID.

	Discussion:

	C: The problem is valid but introducing a key index transfers the problem from the PMKID to the key index, since it's still a unique identifier.
	Q: Could we not solve the same problem by generating transient PMKID in addition to long-term PMKID?
	A: To generate a new PMKID you need to generate a new PMK. This idea proposes to not generate more PMK than necessary. With a key index the PMKID can be kept private. Needs further thought.
	3. **Mechanism of simultaneous changes to SN scrambler seed PN AID and TID** ([11-23-0166r1](https://mentor.ieee.org/802.11/dcn/23/11-23-0166-01-00bi-mechanism-of-simultaneous-changes-to-sn-scrambler-seed-pn-aid-and-tid.pptx)), Chaoming Luo

	Discussion:

	C: Would like to see an analysis of how this proposal works together with other proposals we've heard this week.
	C: Would like to see a separation of the XOR procedure for obfuscation and the generation of AID.
	C: Even today we can do scrambler seed per transmission so the proposal to sync could be overloaded in this sense. Would also like to see analysis of this proposal with respect to others.

	**Strawpoll:** Do you agree 11bi should incorporate the proposed method described below? Request AP to assign or preassign a new AID whenever the associated non-AP changes OTA MAC address?

	Yes: 6
	No: 7
	Abstain: 4
	Need more information: 10

	**Strawpoll:** Do you agree 11bi should incorporate the proposed method described below? Use the following method to obfuscate TID, SN, scrambler seed, PN whenever the associated non-AP changes OTA MAC address: STA and AP compute locally a common random number (RN) using the new OTA MAC address and derive OTA\_TID and OTA\_PN: RN = Hash (OTA\_MAC || IV), IV is a key derived from PTK. OTA\_TID = TID ⊕ RN(0,3) OTA\_SN = SN ⊕ RN(4,16) (TBD) OTA\_SCRAMBLER\_SEED = SCRAMBLER\_SEED ⊕ RN(17,24) OTA\_PN = PN ⊕ RN(25,73)?

	Yes: 1
	No: 6
	Abstain: 2
	Need more information: 17
5. **Administrative**
	1. **Timeline discussion**There was discussion on the timeline. A new timeline will be made available in slide 23 of the updated agenda slide deck (11-23-0189r7).
6. **Any other business**

No other business
7. **Chair declares the meeting adjourned at 14:58 local time.**