IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Minutes Mixed Mode **Interim Session 13-18 Nov** 2022 |
| Date: 2022-11-24 |
| 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 13-18 November 2022. The on-site location for the meeting was Bangkok, Thailand. "Local time" refers to local time in Bangkok, Thailand.

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 14 November 2022, 16:00 local time.**

Chair calls meeting to order at 16:01 local time.

Agenda slide deck: [11-22-1701r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1701-00-00bi-november-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 11-22-1701 (slide #18)**
	1. Agenda approved by unanimous consent (10 remote participants, 11 in-room)
5. **Administration**
	1. **Motion #27:** Approve the minutes for:

2022 July 802.11 Electronic Plenary: [11-22/1648r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1648-00-00bi-september-interim-session-minutes.docx),

TGbi Teleconferences: [11-22/1780r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1780-00-00bi-teleconference-minutes-13-october-2022.docx) (13 Oct), [11-22/1968r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1968-00-00bi-teleconference-minutes-3-november-2022.docx) (3 Nov)

Moved: Stephen McCann

Seconded: Po-Kai Huang

Approved by unanimous consent (10 remote participants, 11 in-room)

1. **Technical Presentations**
	1. **Encrypted Information Element for Obfuscated Beacon (**[**11-22/1882r0**](https://mentor.ieee.org/802.11/dcn/22/11-22-1882-00-00bi-encrypted-ie-for-obfuscated-beacon.pptx))**,** Stephane Baron (Canon)

	Proposal is to introduce a container for information elements that allows for the encryption of information elements.

**Discussion:**

**Q:** What kind of information do you want to encrypt?
**A:** There are two types of information elements: elements that are needed to associate and they need to be in the clear, and elements that do not, and they can be in this container.
**Q:** I don't understand why you've put by default the Element ID Extension outside of the container? If you communicate which amendments you implement, that also entails communicating your capabilities.
**A:** Ah no, the Element ID Extension is for the container, it's not for capabilities.
**Q:** I'm understanding requirement 50 as wanting a new type of Beacon frame that is fully encrypted?
**A:** We are trying to avoid the situation where a beacon needs to be decrypted every time it's received. You can have two containers as well: one which changes, one which remains the same and doesn't need to be decoded again.
**Q:** If we put security headers, MIC headers, etc this proposal could lead to a lot of over-head with lots of containers, surely? Non-AP STA already don't check every beacon so there is no risk of decrypting every beacon if we think of current power-saving strategies.
**A:** The point here is to introduce a container for many information elements, grouped so that those that don't need to be decrypted every time a beacon is checked don't have to be.
**Q:** I'm not sure if defining multiple of these element IDs are necessary if we are anyway defining a new Beacon frame? Have you simulated the overhead introduced by this scheme? This would help me understand the situation better.
**A:** I don't have this at this time. We can discuss offline.
**Q:** Is there a minimum byte size for the encrypted part, or can it be any size?
**A:** It could be as small as one byte of course, but in this case it would not be very practical. In that case you probably want a different strategy.
**Q:** My concern was that a smaller container size would make the encryption scheme more vulnerable, and whether a minimal container size is necessary to protect the robustness of the encryption?
**A:** We could make calculations on this. But padding can be introduced to mitigate this problem.
**Q:** Is the padding generic or static?
**A:** The non-AP STA does not need to know the padding even, so it can be generic.
**Q:** The hash is there to make sure it's known that the content isn't changed. But then an active attacker knows the container hasn't changed, that the padding hasn't changed, and doesn't that open weakness?
**C:** The issue here is privacy, though, so there is one part where you open the encryption scheme to attack, and another where observing the hash could allow for re-identification of the non-AP STA?
**A:** The core here is to allow the change of hashes and padding when the AP wants that, in order to protect identities of associated STA.

**Strawpoll:** Do you support the specification of an encrypted container information element as described in slide 5?

**Q:** This necessitates an out-of-band mechanism to decrypt the information the first time?
**A:** Yes.

Results: Y 6, N 4, A 6

* 1. **RCM Transition Period (**[11-22-1883r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1883-00-00bi-rcm-transition-period.pptx)**),** Stéphane Baron (Canon)

	Proposal is to determine the transition period for a randomized MAC addressed (the time interval within which two OTA MAC addresses co-exist after a change, for instance when the old OTA MAC address needs to be kept to empty a packet buffer built during its existence, while the new OTA MAC addressed is being assigned to later packets in the buffer) based on Buffer Status Report (BSR). BSR will be calculated only w.r.t. old OTA MAC.

	**Discussion:

	Q:** Is it not easier just to change MAC address when the buffer is empty for distributed interframe space (DIFS)? Just change the MAC address when you next access the medium?
	**A:** That restricts non-AP STA flexibility.
	**Q:** The TA only needs to be assigned when packets are taken out of the queue, right? So why does it need to be assigned before you take it out of the buffer?
	**A:** We should not mandate the non-AP STA to act like this.
	**C:** A more elegant solution might be to assign the TA when a packet is taken out of the queue.
	**C:** That does not solve the retransmission problem.
	**Q:** Doesn't using the BSR mandate some permanence of AID? This could allow cross-change identification w.r.t. other parameters.
	**A:** The BSR is AID agnostic.
	**C:** I don't think this is doable before .11be is finished. If the AP deactivates one link the data is forced to another link.
	**C:** You don't need to avoid correlation of traffic on one link or another link.
	2. **Proposed spec texts for protected version of unicast management frames (**[11-22-1975r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1975-00-00bi-proposed-spec-texts-for-protected-version-of-unicast-management-frames.docx)**),** Po-Kai Huang (Intel)

	Proposal presents updates to current spec text that accommodate for protected (robust) versions of some unicast management frames.

	**Q:** When you say EDP robust, is that a convention for naming things or what does it mean?
	**A:** The frame is protected, so we can call it protected and list the ten frames, or we can name is something else and make a robust (protected) version of already existing frame.
	**C:** We don't have this naming convention. Per amendment we define new frames.
	**Q:** So the mechanism to protect here is what?
	**A:** Starting from protected management frames, we could use the same mechanism.
1. **AoB**None.
2. **Recess 17:47 local time.**

**2nd slot. Thursday 17 November 2022 10:00 local time.**

1. **Meeting called to order at 10:02 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. **Agenda review (**[**11-22-1701r2**](https://mentor.ieee.org/802.11/dcn/22/11-22-1701-02-00bi-november-plenary-agenda.pptx) **, slide #18)**
	1. Agenda approved by unanimous consent (14 participants online, 12 in the room).
4. **Administrative items**
	1. Review of teleconference cadence.

	Four teleconferences to be scheduled: 1 Dec (9AM ET), 8 Dec (10AM ET), 15 Dec (9AM ET), 5 Jan (9AM ET)
5. **Protection against spoof AP (**[11-22-1870r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1870-00-00bi-protection-against-spoof-ap.pptx)**),** Graham Smith (SR Technologies)Presents a solution to the problem of a spoof AP tricking a non-AP STA into sending an association request. Non-AP STA is allocated two addresses by real AP, one for association and one for probes. If real AP receives probe address from non-AP STA, real AP responds with an ID and non-AP STA associates if ID is verified. Real AP then assigns two new addresses to non-AP STA. The probe address of the non-AP STA is indistinguishable from a generic passer-by device to the spoof AP, so the spoof AP cannot supply an ID which can be authenticated.

There are known attacks against this solution.

Discussion:

**Q:** Do you agree that we are identifying the ESS and not the specific AP?
**A:** Yes.
**C:** I see an assumption that these IDs need to be synched across all the regions of an ESS immediately, per non-AP STA.
**C:** Our current requirement specifies that we need an ability to identify a known AP. Randomized MAC addresses are used to mitigate passive tracking. You probably need to think a bit more about this in 6 GHz though, where wild card SSIDs are not permitted.
**C:** The attack is more practical than this presentation submits. If the probe address does not change, you simply record the last probe request frame when the target leaves their known BSS, and then you have the probe address and can use it to acquire the authentic ID.

**Chair:** The queue is empty.
6. **Timeline discussion**There was a discussion on the timeline.

**Strawpoll:** With reference to the TGbi timeline:
 A. Keep current timeline until January 2023 meeting
 B. Make timeline changes shown on screen

Result: A: 6, B: 14, No answer: 5 (25 people present, on-site and virtually)

**Chair:** I will introduce a tentative comment collection for March 2023, and shift our letter ballots and re-circ forward to July 2023 and November 2023 respectively. We can return to this topic in January 2023.
7. **AoB.**

	1. No AoB.
8. Chair adjourned the meeting at 11:54 local time.