IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Teleconference Minutes December 07th 2023 |
| Date: 2023-12-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Stéphane Baron | Canon | Cesson-Sévigné, France |  | Stephane.baron@crf.canon.fr |

Abstract

This document contains the minutes for the IEEE 802.11bi task group meetings that took place Thursday December 07th.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**December 07th:**

**Chair: Carol Ansley, Cox Communications**

**Secretary: Stéphane Baron**

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

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

Chair calls meeting to order at 10:02 ET.

Agenda slide deck: [11-23-2162r0](https://mentor.ieee.org/802.11/dcn/23/11-23-2162-00-00bi-agenda-for-dec-telecons.pptx):

1. Reminder to do attendance
2. Review of policies and procedures.
	1. IEEE individual process slides were presented.
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 policy and participation rules.
	1. No questions
5. **Discussion of agenda 11-23-2162r0 (slide #15)**
	1. Discussion on agenda

No discussion

* 1. Adoption of agenda by unanimous consent (10 participants).
1. **Administrative**
	1. Upcoming teleconference meeting times:
		* Dec. 14th 2023: 10:00 to 12:00 EDT
		* Jan. 4th 2024: 10:00 to 12:00 EDT
		* Jan. 11th 2024: 10:00 to 12:00 EDT
2. **Technical Submissions**
	1. [11-23/1876r1](https://mentor.ieee.org/802.11/dcn/23/11-23-1876-01-00bi-mac-change-discussion-irm.pptx) – Epoch start time setting – Stéphane Baron

Stéphane presents briefly the contribution already presented during the November F2F and then present the straw polls not run in November due to lack of time.

* + 1. Discussion

**SP#1** requested by Stéphane Baron:

**SP#1 initial text**: “*Do you support that Epoch’s start time of all non-AP STA affiliated to a single non-AP MLD are aligned in time?”*

Discussion:

Q: Why do you need to change all parameters of each link at the same time?

A: In fact, the problem hidden behind is the AID value. Today, an MLD has only one AID this is nor a per link value. So, if a link changes its parameters using the new AID and still use old AID on other links, the correlation is easy for an eavesdropper and the change is useless.

**SP#1 results**: Y:8 / N:1 / Abstain :2

**SP#2** requested by Stéphane Baron:

**SP#2 initial text**: “*Do you support using a time reference as input for the generation of the CPE parameters of this Epoch?”*

Discussion:

Q: What do you mean by “time reference”, is it a TSF counter value?

A: To be clear, yes, I have in mind to use a TSF counter value. I can indicate it in the SP text.

Q: I have an issue with the current wording. I cannot vote yes to this since some parameters may have different generation method. For instance, I don’t think AID will be randomly generated based on a TSF counter.

A: for me, the TSF value is used to generate the parameters that are generated using a pseudo random generation. This SP do not address other kind of parameters like AID.

Q: Why do you want to use the time rather than the iteration number? Iteration number is much simpler, and in existing random generation we do use the time currently.

A: I think the iteration is much weaker. It is easy to determine the iteration by noticing a change of a lot of stations. But the exact value of that change time cannot be easily determined by an eavesdropper since the parameters used for this generation are send in an encrypted manner. In addition, a TSF counter has much more bits than an iteration counter.

**SP#2 final text**: “*Do you support using a time reference (TSF counter value) as input for the generation of the CPE parameters of this Epoch?”*

**SP#2 results**: Y:6 / N:1 / Abstain :4

**SP#3** requested by Stéphane:

**SP#3 initial text**: “*Do you support that Group Epoch start Time (GET) is based on a fixed frequency (GEI) with a limited pseudo random variation.”*

 ***GETn+1=Tn+1 + ∆Tn+1+ RefLink Offset***

 *with:*

 *Tn+1=T0+ ((n+1) x GEI)*

 *∆Tn+1 = PRF-128\64(GTK\*, “ERCM”, Tn+1) mod (Time range)*

 *GTK\* derived from GTK*

 *RefLink Offset = offset of the TSF counter of the current link compared to the Reference Link.”*

Discussion:

Q: Editorial question; GET is ok but you have no definition of the GEI here, can you replace GEI by Group Epoch Interval?

A: ok, thank you.

Q: This is a very complex SP, with lots of detail. I am afraid I cannot answer now. I agree on the general direction but need time for the details.

A: Ok, I can remove the details of the computation for now and see the opinion of the group on the general direction. Then I can come back to discuss details.

**SP#3 final text**: “Do you support that Group Epoch start Time (GET) is based on a fixed Group Epoch Interval with a limited pseudo random variation?”

**SP#3 results**: Y:8 / N:0 / Abstain :3

Presented propose to run SP# 5 before SP#4 since it is very similar but for Individual Epoch.

**SP#5** requested by Stéphane:

**SP#5 initial text**: “*Do you support that Individual Epoch start Time (IET) is based on a fixed frequency (IEI) with a limited pseudo random variation ∆T.*

 *I****ETn+1=ITn+1 + ∆Tn+1 + RefLink Offset***

 *with:*

 *ITn+1=IET0+ ((n+1) x IEI)*

*(CPE\_PARAMn+1, ∆Tn+1) = PRF-M\L (PTK\*, “ERCM”, ITn+1)*

 *PTK\* is derived from the PTK*

 *RefLink Offset = offset of the TSF counter of the current link compared to the Reference Link.”*

According to previous discussion, the SP text is immediately changed by the author to match previous comments of the SP#3.

**SP#5 modified text:”** *Do you support that Individual Epoch start Time (IET) is based on a fixed Individual Epoch Interval with a limited pseudo random variation?”*

Discussion:

Q: Why do you need a pseudo variation in the case of individual Epoch?

A: If 2 different stations have very precise but different Epoch interval, this interval identify the station uniquely. So, by adding a pseudo random variation, you erase this fingerprint.

Q: What happens if group and individual Epochs have very close starting time?

A: on slide 10 I indicate that if time between next Individual and Group epoch start time is lower than a “TBD” time (e,g. 1s), then Individual Epoch is ignore. I can add this as note if this ok for you.

A: yes, this is ok.

Q: I would propose a more generic note indicating: “interaction between Group and Individual Epoch is TBD”. Because we don’t know how to handle overlapping Epochs for instance.

A: Agree. I take your proposal for now and let’s discuss the details later.

Corresponding note is added to the SP text by the presenter.

**SP#5 final text**: *Do you support that Individual Epoch start Time (IET) is based on a fixed Individual Epoch Interval with a limited pseudo random variation?*

*Note: Interaction between Group Epoch and Individual Epoch is TBD*.”

**SP#5 results**: Y:7 / N:0 / Abstain :3

**SP#4** requested by Stéphane:

Discussion:

C: Many different pseudorandom functions exist that may be used here, so we need to study them and the required output size for instance. So, it is too early to run such SP.

A: Agree, let’s discuss those detail later.

C: We can also define a specific function for this purpose.

A: I think we already have the function we need among existing ones. We should be very cautious if we want to introduce a new pseudo rando generator.

**SP#4 is deferred upon author request.**

No more questions.

* 1. [11-23/2098r2](https://mentor.ieee.org/802.11/dcn/23/11-23-2098-02-00bi-frame-anonymization-fa-normative-text-for-11bi.docx) – Frame Anonymization (FA) normative text for 11bi -- Philip Hawkes

Presentation is deferred. To allow discussion and integration of previous SP results.

No other questions.

1. **AoB**
	1. No other business.
2. Chair adjourned the meeting at 11:21 EDT.

**Attendance**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbi | 12/7 | Ansley, Carol | Cox Communications Inc. |
| TGbi | 12/7 | baron, stephane | Canon Research Centre France |
| TGbi | 12/7 | Ficara, Domenico | Cisco Systems, Inc. |
| TGbi | 12/7 | Halasz, David | Morse Micro |
| TGbi | 12/7 | Hawkes, Philip | Qualcomm Incorporated |
| TGbi | 12/7 | Ho, Duncan | Qualcomm Incorporated |
| TGbi | 12/7 | Huang, Po-Kai | Intel |
| TGbi | 12/7 | Mutgan, Okan | Nokia |
| TGbi | 12/7 | Nezou, Patrice | Canon Research Centre France |
| TGbi | 12/7 | Sam, Harvey | Broadcom Corporation |
| TGbi | 12/7 | Yee, Peter | NSA-CSD |

 |  |  |  |
|  |  |  |  |