Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, June 14, 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-6-14 |
| 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 June 14, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting June 14, 2022 10.00 to 12.00 ET**

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

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

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

**Secretary: Peter Yee, acting**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 10:03 a.m. EDT.**

Agenda slide deck [11-22/0897r01](https://mentor.ieee.org/802.11/dcn/22/11-22-0897-01-00bh-agenda-tgbh-2022-june-14.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
	+ Reminder: Comment Collection on D0.2 closes on June 29
* Issues Tracking: [11-21/0332r30](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-30-00bh-issues-tracking.docx)
* Contributions (slide 16)
* Next meetings:
	+ June 21 and 28 10:00 ET

Any comments? None

Any objections to agenda? - None

Agenda accepted unanimously.

1. **Organization topics**

The Comment Collection is now under way and closes on June 29.

1. **Issues Tracking**

Chair noted that the Issues Tracking document is at r30 but there is a new contribution branch that hasn’t quite resolved. It will be discussed during today’s session.

1. **Issues Tracking Update**

Jay Yang presented [11-21/0332r36](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-36-00bh-issues-tracking.docx), his latest update to the Issues Tracking document.

Since the previous version, text has been added to sections 4.1, 4.2, 4.8, and 4.26.

Q – There are control systems that track MAC addresses as part of their probes. How are RCM STAs recognized? (Section 4.1)

A – These STAs use fixed MAC addresses for this use case.

Q – (Section 4.26) Why is “shall” used in an issues tracking document?

A – Change it to “is”.

Q – Does this version of the document become the accepted task group version?

A – That’s the question to the group.

Q – As we keep adding to and editing the issues tracking document, is the goal to feed some of this back into the draft? When is this document done and we declare that it’s more important to get text into the draft?

A – That too is a question to the group, but other than Jay and his co-author’s input, there has not been much input. I’m assuming that that means the group is happy with the document. The document is meant to be helpful. I’m of the opinion that going forward, efforts should be focused on the draft.

An r37 of the document will be posted with the discussed changes. There is no formal ratification needed for the document, but it will be used as the basis for any further changes.

Q – Can we just accept all changes in the document so that it’s clean and readable?

A – That makes sense. R37 will be posted with everything incorporated.

1. **MAAD MAC Outline**

Graham Smith offered [11-22/0737r03](https://mentor.ieee.org/802.11/dcn/22/11-22-0737-03-00bh-maad-mac-outline.pptx).

This is a clarifying presentation of the MAAD scheme.

1. **Identifiable Random MAC Address IRMA – 3**

Graham Smith also offered [11-22/0894r00](https://mentor.ieee.org/802.11/dcn/22/11-22-0894-00-00bh-irma-3-presentation.pptx), to be discussed together with the previous presentation.

This is like MAAD, but with the STA setting the address to be used the next time it associates.

Q – Is there a mechanism for the AP to tie the current IRM address to the previous IRM address?

A – That is a function of an AP list function. An AP could keep a historical list, but there’s no real reason to do so.

Q – Your proposal uses just one MAC address, against WFA requirements to use different addresses in probes. Could you make your proposal more secure by doing this?

A – Is this for each probe request?

Q – In pre-association, a STA can send many probe request frames. Also, in post-association. But each frame should have a different MAC address.

A – The STA changes its address for each association.

Q – Think of a STA that always connects to the same AP, but probes with a different MAC address. Your proposal requires a fixed MAC address in the probe request.

A – I’m not understanding this question.

C – I think the question is, what address does it use in probes?

A – If it wants to be recognized, it uses an address the AP will recognize. If not, it can use any random address. For association, the STA will definitely use the address that the AP will recognize.

Q – Are these directed probes or broadcast probes?

A – These are directed probes, if you want the AP to know who you are. In that case, you use the address the AP will recognize. If you just want to know if the AP is there, you can use any address.

Q – Why doesn’t Graham want to run straw polls [that are included in the slides]? I’m interested in the answers.

A – The reason that I’m not running them is that they are somewhat similar to the ones run during the last meeting. They might be run at the next teleconference.

1. **Use case further discussion and rule-based Random MAC-Identification proposal**

Okan Mutagan (Nokia) showed [11-22/0818r03](https://mentor.ieee.org/802.11/dcn/22/11-22-0818-03-00bh-use-case-further-discussion-and-rule-based-random-mac-identification-proposal.pptx).

This proposal, like MAAD and IRMA, tries to identify the STA based on the probe request. Today, only versions 2 (slide 10 and 11) and 3 (slides 12 and 13) of the proposal are the focus. It uses a tag to ensure that both sides have the same idea of the random MAC address (RMA). The versions differ between how they generate RMAs.

Matching text can be found in [11-22/0888r01](https://mentor.ieee.org/802.11/dcn/22/11-22-0888-01-00bh-proposed-text-for-rule-based-random-mac-identification.docx). It was briefly introduced to show how it aligns with [11-22/0818r03](https://mentor.ieee.org/802.11/dcn/22/11-22-0818-03-00bh-use-case-further-discussion-and-rule-based-random-mac-identification-proposal.pptx).

Q – You are using AES-CTR mode, the most fragile mode possible. All of the data is sent in the 4-way handshake. Why not use AES-CBC or AES-SIV that will not be as fragile? Why did you choose CTR mode?

A – With the other parameters remaining the same in the RMA calculation, only the counter was available to vary the input to the algorithm. The remaining input parameters remain fixed.

Q – You would have that property if you used with other modes. CTR is usually used with other modes that provide integrity. Since all of this stuff is sent by the AP, what’s the point of doing all of these calculations? This sounds like network-assigned ID, except with more blobs and calculations occurring.

A – Network-generated ID and MAAD send sensitive information. This proposal just sends parameters and lets both sides generate the sensitive information. The keys would have to be cracked in order to derive keys and tags. I don’t think in the network-generated ID solution that the blob covers the probe request. It’s only a solution once the 4-way handshake is in play.

Q – You said that you could keep changing the MAC address. That has other implications and is being discussed in TGbi. The solution goes beyond the problems that MAC address randomization is causing to operational systems.

A – Are you asking whether this should be covered in TGbi?

Q – I meant the part where you are changing it during the association. I’ll need to look at that again.

Q – Was that in the text or in the PowerPoint?

A – I thought it was in the text.

Q – NOTE1 (in 888), once it is set up, it doesn’t need to be done again. But if we have to do the set up on each association, as the note suggests, this is quite a burden on a busy AP. Have you looked into how much work this requires? It was a criticism of the first IRMA scheme. I had thought it was done once. Why did you change to per-association setup?

A – We could have multiple RMAs, each used for different purposes. Yes, there’s a cost to the computations. The current draft uses AES-SIV for each STA for each association. These are needed to be more secure, robust. In our proposal, only the counter is adjusted, so there’s not much above the cost of AES.

Q – I thought your scheme had not run the calculations so much, that was what I meant.

A/Q – The rule-based scheme we used overlaps with the previous versions of IRMA. Those supported different MAC addresses on a per-probe basis, right?

C – Yes. The debate is how often these get updated.

C – Theoretically, we don’t have to use the tag at all, as long as both sides generate the same RMA. Sending the tag helps both sides to ensure they have done so.

Q – The use of the nonce is to generate “lightness”[?]. It should only be used once. Here, you are using a fixed nonce. That seems to be a problem. The use of the counter – how do we ensure that it is in synch on both sides? Counters go out of synch with each other fairly often and fairly easily. What’s the logic to reset the counter to the same state. How is the nonce communicated between AP and STA?

A – All of these values (tag, nonce, seed) are sent in the 4-way handshake, message 2. Counter also helps the STA tell the AP how many RMAs it generated, because there’s only a single tag regardless of how many RMAs were generated. Sending the counter helps with synching.

Q – So, counter is synched and communicates the number of RMAs?

A – Correct.

Q – If the nonce is fixed, then don’t call it a nonce. Call it random value. The receiver should be able to tell that a nonce was reused. We seen problems with nonce reuse.

A – The nonce is per association.

Q – Sure, but the definition of a nonce is a value used only once. I’m not sure about the security of a nonce used repeatedly with only the counter varying in AES-CTR(K1, Nonce||counter, Seed).

A – As Dan indicates (in the comments), the nonce and counter are used together. So, there’s no real reuse of any value.

Q – The counter in the 4-way handshake is the number of RMAs, it’s not actually one of the counters for AES-CTR. The counter used in the computation is a different value (starting at zero and incremented by one) up to the counter value sent in the 4-way handshake. Is that correct?

A – Yes, that’s what is meant.

Q – In the block diagram (in 888), RMA1 is used in the probe, RMA2 is used to associate, and RMA3 is used for data frames. That last one is a TGbi solution, not a TGbh solution.

A – Yes. We don’t really talk about the RMA3 part in regard to TGbh, but we think our solution is applicable to both task groups.

Q – How many bits are added to the 4-way handshake. It’s starting to look like a lot.

A – Figure 12-49 shows 68 bits. There’s always a trade off between privacy and overhead. We can decrease these numbers, if desired.

Q – Question to the group – how do we want to proceed with the supplied text?

A – There’s no problem with having multiple solutions (look at power save). Choose the one that works for you. Whether there’s a preference for the STA or AP to give an ID, do we need to restrict ourselves. The more the merrier and let the market decide. Unless you want to say, “no more and that’s it”, put us out of misery and have a vote on that now.

A – That’s the question - how many solutions and scenarios does the group want to support. I’m looking for thoughts now or perhaps for the next meeting. If we have multiple mechanisms, that will need to be negotiated. We will need to think about how they work together or interact.

A – How many uses cases we want to cover plays a part in this decision. If we want to focus on probe identification, we need further proposals or enhancements to the current proposal.

C – Hopefully, updates to the issues tracking document is helping our thinking about the use cases.

**Meeting adjoined at 11:44 a.m. ET.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 6/14 | Andersdotter, Amelia | Sky UK group |
| TGbh | 6/14 | Ansley, Carol | Cox |
| TGbh | 6/14 | Baron, Stephane | Canon Research Centre France |
| TGbh | 6/14 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 6/14 | Harkins, Dan | HPE |
| TGbh | 6/14 | Lu, Liuming | Guangdong OPPO Mobile Telecommunications Corp.,Ltd |
| TGbh | 6/14 | Lumbatis, Kurt | CommScope, Inc. |
| TGbh | 6/14 | Mutgan, Okan | Nokia |
| TGbh | 6/14 | Nezou, Patrice | Canon Research Centre France |
| TGbh | 6/14 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 6/14 | Petrick, Al | InterDigital |
| TGbh | 6/14 | Sam, Harvey | Broadcom Corporation |
| TGbh | 6/14 | Sevin, Julien | Canon Research Centre France |
| TGbh | 6/14 | Smith, Graham | SRT Wireless |
| TGbh | 6/14 | Smith, Luther | CableLabs |
| TGbh | 6/14 | Thakur, Sid | Apple |
| TGbh | 6/14 | Yang, Jay | Nokia |
| TGbh | 6/14 | Yee, Peter | NSA-CSD |