Minutes IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IEEE 802.11 TGbh Meeting Minutes, December 1, 2022  Randomized and Changing MAC addresses (RCM) | | | | |
| Date: 2022-12-1 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Stephen Orr | Cisco | New York |  | sorr@cisco.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh telecon meeting of December 1, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting December 1, 2022 7:00 p.m. to 9:00 p.m. ET**

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

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

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

**Secretary: Peter Yee**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by the Chair at 7:03 a.m. EDT.**

Agenda slide deck [11-22/2084r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1735-00-00bh-agenda-tgbh-2022-oct-11.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 (see Backup slides)**
  + Sept to Nov teleconferences: Tuesdays, every other week, 9:30-11:30 am ET (this time slot)
  + Timeline reminder (slide 20)
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Results of Comment Collection on D0.2:** [**11-22/0973r13**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-13-00bh-cc41-comments-against-d0-2.xlsx)
* **Motions record**
* **Contributions**
  + [11-22/1329r10](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-10-00bh-cid-resolutoins-for-12-2-11.docx) – CID resolutions for 12.2.11 (Kurt Lumbatis)
  + Enhancement of RCM (Okan Mutgan)
* **WBA liaison response**

Any comments?

Any objections to agenda? [None] – Approved

1. [**11-22/1802r1**](https://mentor.ieee.org/802.11/dcn/22/11-22-1802-01-00bh-enhancement-of-rrcm.pptx) **– Enhancement of RRCM (Okan Mutgan)**

* Recap of RRCM Slide 2: discussed Validation Information Element
* VIE should be constructed using RMAK
* Slide 5 construction of VIE
  + AES-128-CMAC used to compute MIC
* Slide 6 – construction is similar to BIP MPDU
* Q: Does the key change or is it constant?
* A:It changes in every association
* C: The key changes and you advertise a key derived function in the IE (called a MIC in this case)
* Q: How is this different than IRMA?
* A: The difference comes from the hash value (VIE) – you don’t know the RCM in the header, however it checks the VIE, it goes to the database that matches the hash value of the VIE to determine the identity.
* C: Isn’t this exactly what IRMA does? If you have 1000 STAs, you may have to do 500 calculations before you have a match.
* C: The spoofing and copying according to TGbi aren’t seen as problems.
* C: IRMA totally depends on the IE and not the header which is a drawback and adds search complexity. The difference here is if you use the RMA and the VIE you can map it instead of search for it in the database.
* C:If you stored the RMA and all this stuff, you should just use MAAD.
* C: RRCM gives you the ability to generate multiple RCMs
* Chair: These seem to be coming together, maybe there should be a table showing difference/similarities
* Q: Can you explain how to use this?
* A: Just attach the VIE to the payload.
* Q: Is this competing with the current draft?
* A: They can work together or be combined.
* Q: This seems to be a heavy operation for an AP – to do all these calculations. Concerned that it will take AP resources and time.
* A: Do not agree with the complexity, it is a straightforward computation.
* Chair: I think you are asking questions about RRCM not the enhancements.
* A: Enhancements are one piece, the question is how will it be used
* Chair: Doc 818/r4 is the proposal of how it works
* Chair: we need a comparison to keep things straight
* Q: How does the STA select the MAC it will use?
* A:Both AP and STA will use the Counter and Seed to generate the RMAs. The counter determines how many RMAs will be generated.
* Q:How do we know what address to use?
* A: In bh we assume the SSID doesn’t change
* C: Spoof AP thing – turns out that it isn’t a problem. What are we trying to solve here?

1. **ID Encoding**
   * **C:** variation on a theme. If the ID was not encoded it is identical to MAAD. First assoc you are given an ID and then you put it in an IE on subsequent associations.
   * **C:** Not clear what IE is being referred to.
   * **Q:**Which HW currently supports HPKE for encrypt/decrypt?
   * **C:** The first bullet: “If needed for some use cases” IF you don’t encrypt you associate, given and ID and stick it in an information element. This is exactly like MAAD expect you are using an IE vs MAC address.
   * **C:**Lets list what we are trying to solve…

Chair – what are the options in front of us. There are a lot of similarities and little subtle differences. Which ones are in our scope.

Q: Why did we have the 7PM call? There are only 9 on this call and we usually get 13-15.

Chair: We will talk about that during our next call. We were going to try this as an experiment – we will have this discussion.

Q: If Jouni can’t make the next call and all our technical discussions are stalled – should we have the next call.

Chair: We will find out

**Meeting adjoined at 8:30 p.m. EDT.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 12/1 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 12/1 | Henry, Jerome | Cisco Systems, Inc. |
| TGbh | 12/1 | Levy, Joseph | InterDigital, Inc. |
| TGbh | 12/1 | Mutgan, Okan | Nokia |
| TGbh | 12/1 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 12/1 | Sevin, Julien | Canon Research Centre France |
| TGbh | 12/1 | Smith, Graham | SRT Wireless |