Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, 28 June 2021Randomized and Changing MAC addresses (RCM) |
| Date: 2021-06-28 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technologies | Sunrise, Florida |  | gsmith@srtrl.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11 bh telecom Interim meeting 28 June 2021.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer given by the presenter

C- proceeds a comment

**Meeting June 28, 2021 1.00 to 3.00 pm ET**

**Chair: Mark Hamilton**

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

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

**Secretary: Graham Smith (SRT Wireless)**

**The teleconference was called to order by Chair 1.03 hrs. EDT,**

Agenda slide deck 11-21/0975r0

Chair noted that the Editor position is still vacant and asked for volunteers.

**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 also Backup slides):**
	+ PAR/CSD: [https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8770](https://development.standards.ieee.org/myproject-web/public/view.html); [11-20/1117r5](https://mentor.ieee.org/802.11/dcn/20/11-20-1117-05-0rcm-rcm-sg-proposed-rcm-csd-draft.docx)
	+ Timeline estimate
* **Issues Tracking:** [**11-21/0332r8**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-08-00bh-issues-tracking.docx)
* **Contributions:**
* **Next meetings: Plenary session, July**

The Chair reviewed the agenda. Any comments? None.

The proposed agenda was adopted without objection.

Attendance is listed at end of the Minutes.

Any discussion or comments on the back up material? Timeline? None.

Chair observed we are getting close to working on draft material and on solving identified problems.

1. **TGbh Issues Tracking document: 11-21/0332r8**

Use Cases

Previously discussed Use Case, 3.6.2 from 19/1442r9

**Infrastructure (home or enterprise): Probes are randomized, even to/with associated SSID**

Any more discussion on this? None

**Next topic from the TIG report is 3.8**

##  Rogue detection in infrastructure networks

*A managed WLAN network may desire to detect rogue, un-authorised access points and/or client stations operating in its service area. One such rogue detection mechanism entails monitoring for users associated to access points which are not known to be part of the managed network. The MAC addresses of the known APs are kept in a database, and the medium is monitored for Beacons or other broadcast traffic from, or non-AP STAs’ traffic to, APs not on the known AP list.*

*Non-AP STAs could also be listed on a known client list, by MAC address, and thereby unexpected/unwanted client devices in the service area can be detected, by detecting unknown MAC addresses.*

*When a rogue AP or STA is detected, appropriate action (such as contacting the owner) can be taken to resolve any issues such as interference with the operation of the managed WLAN.*

Thoughts on this Use Case?

Discussion took place, Chair added text to the document during discussion:

C – An important topic and is a problem. Not sure there is much we can do about it however.

Q – Evil twin APs I see but struggle to see problem of a rogue STA?

A – In enterprise, only expect authorized STAs. Can track attackers from the outside, maybe by RSSI, but if a new MAC comes up, then that is a warning. Hence, with RCM any valid STA could be an attacker because no way to tell one from the other.

C – Still don’t see why this is a problem as authorization takes place.

C – Do not understand “rogue device” based only on MAC address. Cannot recognize anyone solely on MAC address.

A – Issue is control, have a whitelist of devices, match MAC addresses against list and where they are. A rogue may spoof MAC of known “good” device, then detected that new MAC address is from different area. Secure areas, for example, so we know where the STA should be.

C – Surely you need a credential?

C – Point is you do not want to see a MAC address you do not know. An entire section of building may be secured. Noting as devices enter and leave area.

C – Do not understand use case. Devices should work everywhere.

C – Distinguish between rogue client and soft AP. Soft AP will raise alarms, as bypassing the network.

Q - If same MAC when associating to same AP/network isn’t this sorted out? Is the only problem when MAC changing periodically?

A – Have laptop and soft AP and share connection. Next time you come back now have same MAC but this is not the MAC of your laptop.

C – Is soft AP another use case? I was referring to the “standard” case where STA keeps MAC address every time. Problem only if STA decides to change MAC address even though associated which should not happen.

Q – How do you decide original MAC address to use in order to be on the whitelist?

C – What kind of agreement can occur in enterprise not to open up a soft AP?

A – Part of a written agreement. Then not part of 802.11 base. Don’t think we have soft AP concept.

C – There are many hooks for higher layers in our spec. This case (soft AP) may or may not have the hooks, but we could add hooks.

Q – If associated to an enterprise network you should not operate a soft AP, is that the sort of statement?

C – An agreement, verbal or written may exist that no user will bring up a soft AP.

C – But there are devices that are expected to work everywhere, Wi-Fi speakers for example.

C – Same as not allowed to use a camera. Only written. Not allowed to bring in any device with recording ability, etc.

C - Must be configured with the application set to Off. Or ban device.

C – We do need to connect this back to RCM. Maybe this simply makes it worse if RCM?

C – What functions do not work if RCM is operating? So rogue STA is impacted. We only need to identify that that problem is made worse. Just need to recognize that there will be an impact.

C – Can we state what the impacts are, and what we could do about it?

C – System should be able to recognize that the client is not known. Once associated, then OK?

C – Solving RCM condition of providing a secure ID, then that may allow this use case to function correctly.

C – Depends if triggering on probes or only on association? Do “rogue probes” matter?

A – Yes, today unknown probes will trigger reaction. So only way to recognize an unauthorized device is via its probes.

C – If directed probe should use the known MAC address for that network, then it works. If unknown do you wait to see if it associates?

C – Important that devices use RCM when broadcasting probes. Some implementations, if response from known SSID, then will do a directed probe with the connected MAC address.

C - When you probe you declare nothing about yourself. Once you get SSID you want, then do a directed probe.

C – In secure environment, you send security personnel if you see a “new” device. You do not have privacy if you are entering a secure area.

C – Solution is simply “device policy”. Configured and permitted devices only.

C – Could be a ‘recommended practice’ solution.

Let’s switch to the “AP Problem”

*Soft AP in an enterprise controlled environment.*

C – Simply not allowed, as this would be detected and action taken.

C - No RCM effect in enterprise.

C - What about issue of Soft APs if their BSSID changes?

C – Soft APs are short lived. Shut down when not needed or if no one associated. Privacy concerns also apply, so keep BSSID randomized.

C – When soft AP up and active it cannot change its BSSID.

C – May need to describe this short term idea and soft AP in the standard?

C – Don’t see a problem. Soft AP likely to be a personal device. If you stop and restart with new BSSID, will not change SSID. Clients always use the SSID only. Even if two the same, one will fail to connect due to password.

Q – Don’t change address when beaconing? Am I now trackable?

A – Devices will automatically tear down if no traffic. Short lived, otherwise battery runs out.

C – 11aq says nothing about (soft) APs. Could add text/recommendations.

Return to problem “onboarding a “known” MAC address (secure environment or controlled), but does anyone know the address?”

C – Rogue detection system in place. If BYOD then not managed based on credentials.

C – Campuses. Lots of devices, PSK passphrase. Do not have ability to identify devices if RCM. A PSK personal problem.

Next Use Case:

##  Customer Support and Troubleshooting

*Service providers are deploying wireless gateways in residential environments. With about two thirds of customer complaints related to WLAN, operators have to be able to provide top-notch technical support when a subscriber faces WLAN-related issues.*

*As an example, a subscriber has 16 devices connected to their 802.11 network. They have set-up different SSIDs for their guests, their kids, and their personal devices.  The subscriber is experiencing connectivity and low performance issue on their wireless network. When they call the technical customer center, the technician is able to identify the MAC address of the faulty device and ask the subscriber to reset its device and reconnect to the wireless network.*

C – How feasible is this with a non-technical user? No one will know their MAC address. Usually just “reset” is the advise.

C – Don’t the devices keep the same MAC in this same network?

C - Problem is that the MAC even if stable, is random, so no way to know which device it is.

C – Device that has an issue, and don’t know which it is. Sending illegal packets for example and changes MAC address, so address changes even while on the call, so can never find it as yesterday had one address and today (on call) has another.

C - Problem is that the MAC even if stable, is random, so no way to know which device it is.

Who is who.

C – Could demand that devices turn of RCM so as to determine who is who.

C – Many providers could be providing service: internet service provider, manufacturer. Mostly basic steps and re-boot are the responses. Automated steps.

C – How can a provider know which device is which as devices on my own network AP are behind the modem?

C – Most service providers will use cloud based systems. With second AP/router in line I don’t know how they will do that.

C – This Use case is focused at residential, is there an enterprise equivalent?

C – Enterprise runs different control. Could change text to cover both?

C – Different to home support case, but maybe similar enough with IT in place of service provider.

Discussion halted due to time.

**Next meeting at Plenary Meeting in July.**

Use cases need cleaning up in document, before we consider specific features for solving.

**Out of time**

**Meeting Adjoined at 2.58pm ET.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 6/28 | Ansley, Carol | Cox Communications Inc. |
| TGbh | 6/28 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 6/28 | Henry, Jerome | Cisco Systems, Inc. |
| TGbh | 6/28 | Hervieu, Lili | Cable Television Laboratories Inc. (CableLabs) |
| TGbh | 6/28 | Huang, Po-Kai | Intel Corporation |
| TGbh | 6/28 | Levy, Joseph | InterDigital, Inc. |
| TGbh | 6/28 | Lumbatis, Kurt | CommScope, Inc. |
| TGbh | 6/28 | NANDAGOPALAN, SAI SHANKAR | Infineon Technologies |
| TGbh | 6/28 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 6/28 | RISON, Mark | Samsung Cambridge Solution Centre |
| TGbh | 6/28 | Shalom, Hai | Google |
| TGbh | 6/28 | Stanley, Dorothy | Hewlett Packard Enterprise |
| TGbh | 6/28 | Wang, Lei | Futurewei Technologies |
| TGbh | 6/28 | Yee, Peter | NSA-CSD |

 Smith, Graham SRT Wireless