IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of Comments Received from China NB during FDIS ballot on IEEE 802.11ah |
| Date: 2019-02-12 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Andrew Myles | Cisco |  | +61 418 656587 | amyles@cisco.com |

Abstract

IEEE 802.11ah-2016 was submitted to ISO/IEC JTC1/SC6 by IEEE 802 for adoption under the ISO/IEEE PSDO Agreement as 6N16663.

The FDIS ballot passed, with a negative vote and a single comment from the China NB. This submission proposes a resolution to the comment.

R1: fixed a number of typos, fixed footer and refined language

R2: added the China NB’s comment for reference

The IEEE 802.11 WG thanks the China NB for their comment in the FDIS ballot, conducted according to the PSDO process agreed by IEEE-SA and ISO, on IEEE 802.11ah.

The China NB’s comment is:

**China NB’s comment**

*IEEE 802.11ah is the amendment to IEEE 802.11-2016, which is a revision of IEEE 802.11-2012. It is an amendment based on IEEE 802.11-2016 as amended by IEEE 802.11ai. China voted against IEEE 802.11 and IEEE 802.11ai during 60-day pre-ballots and FDIS ballots with several technical comments (see comments for ISO/IEC/IEEE 8802-11:2018/FDAmd 1, 6N16794 and 6N15494).*

*It is noted that IEEE 802.11ah mainly extended specifications for PHY and MAC layers. We are glad to see statements to forbid use of WEP (because of its security weakness) in the proposal, and it is noted that there are adaptability revisions on CCMP cryptographic encapsulation. However, this certain proposal still uses the flawed security mechanisms specified by IEEE 802.11-2016 and IEEE 802.11ai. For instance, in Annex B.4.28.1, Robust security network association (RSNA) is clearly stated as one of the compliant terms. There is no further specifications to address problems pointed out in aforementioned documents (6N16794 etc.) regarding flawed security protocols, default using of typical cryptographic algorithms like AES (not including other compliant options), unsecure communication channel issue and so on.*

*If this proposal failed to make up the security flaws in its base standards, there will be flaws in its implementation.*

*China cannot support IEEE 802.11ah to publish as an international standard because all the technical comments on its base standards should be completely solved.*

**China NB’s proposed change**

None

The IEEE 802.11 Working Group would like to inform ISO/IEC JTC1/SC6 that it has decided not to make any changes to IEEE 802.11ah as a result of the China NB’s comment:

* The comment does not propose any explicit changes to IEEE 802.11ah for consideration by the IEEE 802.11 Working Group.
* The comment does not document any validated issues. Rather, the comment generally highlights the same issues the China NB has asserted many times over multiple years relating to the security mechanisms specified in the IEEE 802.11 standard and its amendments. The IEEE 802.11 Working Group have addressed similar issues in previous comment responses liased to ISO/IEC JTC1/SC6. IEEE 802 experts have also participated in many discussions on similar issues over multiple years within ISO/IEC JTC1/SC6. The IEEE 802.11 Working Group continues to believe that the issues asserted in the China NB’s comments are not currently justified by any known evidence.