IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution of Comments Received from China NB during FDIS ballot on IEEE 802.11aj | | | | |
| Date: 20200708 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Andrew Myles | Cisco |  | +61 418 656587 | [amyles@cisco.com](mailto:amyles@cisco.com) |

Abstract

IEEE 802.11aj was submitted to ISO/IEC JTC1/SC6 by IEEE 802 for adoption under the ISO/IEEE PSDO Agreement.

The FDIS ballot passed (N17204) on 26 June 2020, with no negative votes and two comments from the China NB This submission proposes a LS to SC6 with resolution to the comment.

The IEEE 802.11 WG thanks the China NB for their comments (which are not associated with a negative vote) in the FDIS ballot ballot on IEEE 802.11aj, conducted according to the PSDO process agreed by IEEE-SA and ISO. The following text responds to the China NB’s comments.

**China NB comment CN1**

China voted yes and submitted the following comment in 60-day ballot:

*Clause 12.2.2 states “The RSN operations in a CMMG BSS shall be the same as the RSN operations in a DMG BSS.” However, this clause is irrelevant with the subject “Enhancements for Very High Throughput to Support Chinese Millimeter Wave Frequency Bands (60 GHz and 45 GHz)”. Selection and using of security mechanism should NOT be bound with CMMG BSS. Besides, China NB has pointed out the technical problems about RSN mechanism for several times during the past ballots.*

In the response to 60-day ballot comments, IEEE 802.11 Working Group has decided not to make any changes to IEEE 802.11aj.

The reply said ISO/IEC/IEEE 8802-11 defines a default security mechanism for the purposes of interoperability, but implementers are always free to define and use additional methods.

It is welcome for the statement. Accordingly, it is proposed to make this clearer in the text, because currently there is no such clue that other mechanisms can be used by implementers freely.

The comments and proposed changes are clear and reasonable justifications, which should be compelling enough for experts who participated the drafting, and will leave no burden for the implementation.

On the other hand, Chinese experts having participated in the proposing process in IEEE 802.11 TGaj as individuals (or representing some affiliations) and contributed personal ideas, is not a reason for national body to stop presenting reasonable technical opinions during formal ballots, and also it’s not a reason for refusing to accept reasonable opinions according to the ISO/IEEE PSDO Agreement.

IEEE as the A category liaison to ISO/IEC, is obliged to properly handle comments from national members at any stage of the international standards development process, rather than refusing to change the text on the grounds that this stage is a “late stage”.

**China NB proposed change CN1**

To solve the concerns raised by this sentence, it is proposed to change as following:

*The security operations in a CMMG BSS can be the same as the security operations in a DMG BSS. Other security methods and cryptographic algorithms that are defined in ISO/IEC international standards or local regulations can be implemented in a CMMG BSS.*

Or

* + 1. *Delete 12.2.2.*

**IEEE 802.11 WG response to CN1**

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 802.11aj as a result of CN1:

* CN1 is substantially similar to the China NB’s comment in the 60-day ballot. The IEEE 802.11 Working Group’s response is also similar.
* The proposed change replaces “RSN operations” with “security operations”. This change is unacceptable because it replaces something which is specific and well defined with something that is not defined.
* The alternative proposed change of removing the clause completely is also unacceptable because this would mean that the RSN operations in a CMMG BSS would be undefined
* The proposal to explicitly state that other methods can be used to implement security for CMMG is unnecessary because this is easily understood by reading the complete standard. In addition, the proposal is inappropriate in this clause because the general principle applies across the standard and not just CMMG.

**China NB’s comment CN2**

China voted against IEEE 802.11 and its amendments in the past with technical comments (see detailed comments in 6N15494, 6N16794, 6N16982, 6N16983 etc.).

The previous comments pointed out the security problems about IEEE 802.11 (see 6N16794 etc.), such as flawed security protocols, only permitting to use typical cryptographic algorithms like AES (not including other compliant options that are compliant with ISO/IEC international standards and local regulations), unsecure communication channel issue and so on.

If this proposal failed to make up the security flaws in its base standards, there will be secure risks in its implementation. As a consequence, during implementation, China will choose to adopt other security mechanisms that are compliant with local regulations.

**China NB’s proposed change CN2**

None*.*

**IEEE 802.11 WG response to CN2**

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 802.11aj as a result of CN2

* CN2 does not propose any explicit changes to IEEE 802.11aj for consideration by the IEEE 802.11 Working Group.
* CN2 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.