**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **DraftC comment resolution - Compact Frames & RPA - CIDs 497, 507, 508, 509, 619, 629, 512,** |
| Date Submitted | May 02, 2024 |
| Sources | Alex Krebs (Apple)  krebs @ apple.com |
| Re: |  |
| Abstract |  |
| Purpose | To propose resolution for MMS related comments for “P802.15.4ab™/D (pre-ballot) C Draft Standard for Low-Rate Wireless Networks”. |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group or IEEE 802.15.4ab Task Group. It represents only the views of the participants listed in the “Sources” field above.It is offered as a basis for discussion and is not binding on the contributing individuals. The material in this document is subject to change in form and content after further study. The contributors reserve the right to add, amend or withdraw material contained herein. |

Abstract

This submission contains the proposed comment resolutions for 802.15.4ab pre-ballot DraftC.

R0: initial document

R1: added related, previously discussed but unresolved CIDs from DCN 103

# Compact PSDU & RPA

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **CID** | **p.** | **Sub-clause** | **l.** | **Comment** | **Proposed Change** | **Proposed Resolution** |
| Tero Kivinen | 497 | 18 | 7.3.7.1 |  | There is no reason to add Compact frame format, as it is not more compact that normal frames. For example the compact advertising poll will be as:   Octet: 1 3 3 1 variable 2  Frame Type/ RPA RPA Message Message FCS  Compact Frame ID hash Rand Control Content  Using standard frame format with using only destion short address (both assume that devices have already done some association etc, to either get the short address assignment from coordinator, or the identityResolvingKey).   Octets: 2 2 1 variable 2  Frame Destination Command Message FCS  Control Address ID Content   Frame control: Frame type = MAC Command  Frame control: Security enabled = FALSE  Frame control: Frame Pending = FALSE  Frame control: AR = FALSE  Frame control: PAN id compression = TRUE  Frame control: Sequence number supression = true  Frame control: IE Present = false  Frame control: Destination Address Mode = short  Frame control: Source Address Mode = none   As the source address is none, there is no source address, nor source pan id.   As the destination addres is short, and pan id compression is true, so we only have destination short address, and no destination pan id.   In this case the Compact frame has overhead of 10 octets, where the standard 802.15.4 frame has overhead of only 7 octets.   This of course assumes there is only one network in the same area, thus we can leave destination PAN id out, but the compact format assumes that too.   Note, that the PAN coordinator can recognize short addresses it has not given out, thus by seeing such destination addresses, it knows there is devices not part of its network nearby, and knows to avoid to assign those numbers to devices part of his network.   If better support for multiple networks is needed, we can use PAN ID compression set to FALSE, in which case the overhead goes from 7 to 9 octets, which is still smaller than compact format.   In case we use example of Advertising response there is only RPA hash, and no RPA rand, thus the overhead is 7 octets, which is same as standard format.   Using standard format we can use standard features, like destination PAN id, in case we want to get better conflict resolution when there is multiple networks on the area, as then everybody can see whether the PAN id is correct, thus whether frame is for their network or some other network. Also if PAN coordinator sees anybody using same PAN ID and short address not assigned by PAN coordinator, it knows there is PAN ID conflict, thus can change PAN id of its network (this is standard opertion defined in 10.17).   In case security is needed, there is already standard method of doing that, and no special processing is needed.   Also when the privacy addressing is defined in 4ac, the 4ab can use it without modification as it is defined for standard 802.15.4 frames.   Also if there is still issues when frames gets too large, we could take the PHY frame fragmentation from 23.3 and move it to 10.x and define it so it can be used in other PHYs than LECIM DSSS.   I do not see any benefits for adding compact frame format, which uses same amount of octets than standard format and just adds new MAC frame formats offering no benefits.   Using MAC Command frame formats contains 8-bit Command ID, so adding 21 compact frame ID values there is not an problem. | Remove compact frame format, and use standard frame formats. | Reject. (use of compressed/compact PSDU has been agreed on in DCN 23-481r1)  Discussion: The length reduction exemplified in the comment results from reducing the address size from 6 to 2 bytes only for the MAC command frame. Separating the question of RPAs from Compact Frame Format, there is no reason why one frame should use a 6 byte address and the other a 2 byte address for a comparison. If we use an address field of equal length to fairly compare both frames, then the compact frame is 2 bytes shorter than the MAC command. Increasing airtime efficiency is not the only reason for compact frames, but also by overriding limitations of legacy MAC data frames, e.g. the inability to mix plaintext, authenticated, and encrypted and authenticated fields in the payload. See DCN 23-604r0 for more details.  As for the RPA argument "4ac 2-byte addresses are better in some regard than the 6-byte RPAs", that may be true for some applications, but for others not. The two concepts are not interchangeable as we have discussed in previous 4ac sessions: dependence of a central coordinator unit is a strong requirement that may or may not come with privacy implications tbd in 4ac, dependence on frequent resynchronization of OTP lists via secure channel, and unresolved problem of OTP depletion when Initiator and Responder are not connected were among of the differences discussed and the issues still to be tackled.  Frame fragmentation is actually counterproductive as airtime cannot efficiently be quantized into infinitisemal small units. For some applications distributing airtime occupancy over multiple fragments may be preferable, for others defragmentizing airtime occupancy for efficient scheduling may be preferable.  The addition of compact frames to 4ab is not a mandate to abolish the other frame formats. In particular, there is no general purpose compact data frame defined and instead the defined compact frames are meant for carrier coeherent operation with a UWB radio preferably. Therefore there is no harm in adding the compact frame. Additionally, there is extended compact frame address space reserved which can be further enlarged for future  enhancements. E.g. when 4ac turns out to be a great success, e.g. by resolving the #508 issue, additional compact frames can be defined to take advantage of other private address formats or other enhancements. |
| Tero Kivinen | 507 | 64 | 10.38.10.1 | 3 | The text is not really true, as it seems each compact frame also include some form of address in form of RPA Prand, RPA hash, advertiser address, and/or resp address, i.e., there is 3 or 6 octets of exra overhead. In addition to that there is extra message control byte which seems to have only one or two values. Getting rid of the useless compact frame format, and instead of using MAC commands, we can compress the message id and message control to one octet, i.e., encode both those in mac command id, and we can compress the addresses to short addresses. In addition to that we get the privacy for free when the 4ac defines it, and we do not need separate frame types for those cases where difference is only in the addressing (for example there is public start of ranging compact frame which is same as advertising poll compact frame, except the addressing). | Remove compact frame format, and uses standard frame formats. | Reject. Compact frame format is as stated 1-byte header only, everything else is defined on a per message basis. See also #497 |
| Tero Kivinen | 508 | 64 | 10.38.10.2.1 | 13 | The private addresses defined here does not provide privacy unless security is also used, as long as the IRK is not change, any attacker who have knows one valid RPA\_hash, RPA\_prand pair can always repeat that exchange, and only those devices which know valid IRK will respond. This means as long as IRK is not updated, it is trivial for the active attacker to keep track of devices.  So to provide proper privacy against active attacks, the system needs replay protection, which can already be provided if the MAC command frames are used instead of the compact frames. | Use the privacy addresses defined by the 4ac. | Reject. It is true that RPAs do not provide protection against "active polling" privacy attacks. It is unclear how 4ac will solve this problem, but when it has done so at some point in the future, additional compact frames can be added if the group expresses a need for active polling protection. |
| Tero Kivinen | 509 | 64 | 10.38.10.2.1 | 13 | There will be lots of collusions in RPA\_hash, thus there will be need for resolving those conflicts. As there is no PAN id, and most things only use RPA\_hash in the frames, there will be duplicates quite often. This will get worse if multiple IRKs are used, as that means it multiplies the number of valid RPA\_hash values that are accepted. Also this is not function of how many people are in your network, but this is function how many people are in the radio range. Thus having school with 1000 people all in the one room for school wide session will cause collsions in 50% propability if each of the have two IRK and there is two devices for each of their networks (i.e., 2000 devices, each having two IRKs, meaning there is 4000 valid RPA hashes picked at random, thus most likely there is already two that uses the same ones).  Also if there is several tens or hundreds of million of people using the system then there will be collisions in single network, as there will be only 2^24 addresses, meaning that initiator and respoder will have same RPA hash. | Use the privacy addresses defined by the 4ac. | Reject. For a ranging error to occur both an RPA\_hash collision and an OTA packet collision needs to occur simultaneously. The resulting ranging error rate has been calculated as 0.00000016% in DCN 23-126, i.e. 1 ranging error every 726 days.  Discussion: What about "global hash collisions"? OTA packet errors cannot occur for unlimited distances around the word, no detrimental effect results from RPA\_hash collisions in non-interfering PANs. |

# Discussed but no consensus

A close up of text

Description automatically generated

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Idx** | **Pg** | **L.** | **Comment** | **Proposed Change** | **Resolution** |
| Rojan Chitakrar | 629 | 64 | 22 | What is reference [2] and is it a normative reference? If so should be listed in clause 2 (Normative references). AES is widely used in IEEE, please check if the normative reference FIPS Pub 197 included in 802.15.4-2020 already covers the AES-128-ECB. | Please check if the normative reference FIPS Pub 197 already covers the AES-128-ECB, else add the relevant reference in the subclause 2. | Revise. (see #512)  Discussion: Indeed it turned out ECB is not included in 802.15.4me-D01 through the FIPS Pub 197 reference. To avoid an unnecessary increase in receiver complexity by requiring ECB mode implementation for 802.15.4ab devices, the proposed resolution is to use the AES-128 block operation instead which is already included in 802.15.4. |
| Rojan Chitrakar | 619 | 59 | 10.38.8.4.3 | 9 | "NbaPrng( ) which shall be the AES-128-ECB(key, data) function in counter mode as specified in [B2]…". If this is a mandatory requirement, [B2] should be included in clause 2 (normative references). AES is widely used in IEEE, please check if the normative reference FIPS Pub 197 included in 802.15.4-2020 already covers the AES-128-ECB. | Revise. (see #512) |
| Tero Kivinen | 512 | 64 | 21 | The output of the AES-128-ECB is not a integer number, thus you can't take module function out of it. The output of the encryption is the 128-bit bitstring. You most likely want to say something like that RPA\_hash will be rightmost 24 bits of the output of the encryption function. | Define calculations using bit strings. | Revise. Change lines 20-22:  An RPA\_hash is then given by bits 0 to 23 of h(key=IdentityResolvingKey, data=RPA\_prand) where h is the block cipher referred to by AES-128 [B.2.2-4meD01] with an IRK and the initiator's RPA\_prand as input. |

**Discussion:** Clause 9.3.1? Removed integer representation language, as it is irrelevant for how the bits are sent over the air. Discussion over reflector regarding CID 512 suggested there is no consensus on the proposed solution yet. Update after discussion over reflector: Note that the B.2.2-4meD01 refers to FIPS 197 for definition of AES-128, and in FIPS 197 (November 26, 2001) the input/output was defined in Ch. 3.1 as "sequence of 128 bits" and "such sequences will be numbered starting at zero and ending at one less than the sequence length". A newer revision (May 9, 2023) of FIPS 197 states in Ch. 3.1 "A block is a sequence of 128 bits; the data input and output for the AES block chiphers are blocks."