IEEE P802.15

Wireless Personal Area Networks

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | Issues with 802.15.4 | |
| Date Submitted | 17th January 2023 | |
| Source | Benjamin Rolfe (BCA) | E-mail: ben.rolfe @ ieee.org |
| Re: | Revision of 802.15.4 (TG4me) | |
| Abstract | Psudo-random collection of issues found in 802.15.4 while using the standard | |
| Purpose | Support TG4me clean up of the standard | |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend, or withdraw material contained herein. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |

Miscellaneous 802.15.4-2020 Issues

# Introduction

Stuff found when using the standard generally while looking something up, not while explicitly looking for problems. Some are very, very old. Some are the result of not updating the standard when things were added or changed. Some are because we people don’t do what we say and it’s time to admit it and align the standard with reality (in one contributor’s opinion).

Presented by clause.

The title is “issues” not “issues and fixes”. The second part is going to take some work.

# Clause 5

5.3: This is woefully out of date. We should update to reflect the more common uses. It wasn’t too bad in 2006 but things change.

A BASIC device has a single radio interface. A conforming device has at least one radio interface and may implement many radio interfaces (PHYs). We have an implied “one MAC per PHY” which has been somewhat typical now we’re adding MAC features to use multiple different PHYs in coordination.

The most common network topology is peer-to-peer without a PAN coordinator as PAN coordinator is defined in the standards now. Most commonly, only the random access at the MAC layer is used. Short address distribution is done at a higher layer, sometimes by magic and other times by out of band communication. Sometimes short addresses are not used. The legacy association process is seldom used.

The current definition of RFD and FFD is such that most all 802.15.4 devices (even some folks call RFD) are in fact FFDs because they can (and must) communicate directly with other devices. Indeed the indirect communication model is seldom implemented. So most of the time when folks say they have an RFD it isn’t, it might be a light weight FFD. E.g. WI-SUN FAN LFD which is an FFD (does direct communication ONLY) with a subset of the full FAN feature set.

Seems people don’t read or understand the definitions in the standard. The standard definitions are not wrong, just not really useful anymore.

The difference between “coordinator” (an FFD that can communicate directly) and “PAN coordinator” is generally confused. A PAN coordinator is the center of a hub, the only thing non-coordinators can communicate with, owner of a legacy superframe, and so on – things seldom used. The term IS used to mean things like a border router in a mesh which is really a coordinator that takes on the BR role.

Perhaps it’s time we revise the description to make it more clear or even consider clearer terminology better aligned with what people actually do. Or perhaps we strip down some of this in clause 5. Best might be remove the clause.

6.2.5.1 CSMA-CA algorithm

The CSMA-CA algorithm shall not be used for the transmission of Beacon frames in a beacon-enabled PAN, Imm-Ack frames, Enh-Ack frames, or Data frames transmitted in the CFP…

This is largely obsolete. Also not completely correct. And generally ignored. But IMO sending the wrong message in several ways.

It made some sense for the beacon used in a BE-PAN to signal the start of the superframe. Likewise, an Imm-ACK when the ack had to be generated/received within 12 symbol periods. But beacons (even in a legacy BE-PAN) are used for other things, sometimes asynchronously, such as query/response and active scan. And Enh-Ack can carry data and be secured, which means larger than an Imm-Ack with more processing in and out. So it may not fit the model of data+ack being atomic.

Beacons are used for other things. Considered such as active scan and the poll/reply function, which can be done in a BE-PAN too (though of course seldom because BE-PANs so rare – but not extinct completely e.g Echonet). Using CSMA for scan can be helpful and instead of prohibit it we should encourage it.

The reason for NOT using CSMA for periodic beacons used for synchronization is the reduce uncertainty in the transmission time of beacons. Likewise for Imm-ack. It makes sense to allow for that, and less sense to mandate it.

There are a lot of cases where this is a good model (e.g. ranging exchanges where solicit/response should be considered atomic whether data frames or data+ack are used. So CSMA should always be optional. Many times CSMA is not used for random access (e.g. Wi-SUN FAN).

Simplest thing is to delete the sentence.

Then we get to the “CFP”. This prohibition is based on the common mistake of assuming all other devices in the radio SOI are adhering to your schedule. This highly unlikely. LBT can be a benefit anytime there can be other non-coordinated transmitters, which is almost always. It isn’t always useful, but there’s no reason to prohibit it’s use. Prohibition in this case is flat wrong. Probably done to make it easier to figure out how to size slots (if you use CSMA it’s more complicated).

Experience proves that CSMA may be beneficial in scheduled timeslots. TSCH allows it, so this is also in conflict with another part of the standard. Using CSMA may be very useful in scheduled timeslots (what we erroneously call contention free) which exist in various ways in the current standard.

The term “contention free” should be eradicated as false advertising, along with GTS, as when using licensed exempt spectrum there are no guarantees of exclusive access, ever. We could say “scheduled access period” and “dedicated time slot” which are less wrong, at least hinting that our schedule is honored only by a select few users.

Yes many people do not get this and many features of 802 protocols are based on this invalid assumption that all users of the band are coordinated. Lets stop being those people.

6.3.4 Beacon generation

A device shall be permitted to transmit Beacon frames only if macShortAddress is not equal to 0xffff.

This is wrong, and has been for quite some time. It might be ok for the periodic beacon in a BE-PAN but elsewhere just wrong. Also table 6-4 is wrong: For a value of 0xFFFF it says something different from the text.

Actual use of SAs typically have some means to assign and distribute SAs that is outside the scope of this standard. Beacon frames can be use for many things (query/reply, scan) in which out of band SA management may exist and so using SAs in these exchanges saves bits over the air. Since this is commonly done today, we should not pretend it’s still 2003 😊.

The device is not associated and, therefore, shall not perform any Data frame communication.

Which is **clearly not the behavior in most implementations since 15.4 association is seldom used**. Short address is not used the way it was intended in 2003. Beacons are used by several MAC features when short addresses may not be used (thus the value would be the default according to table 8-94). And all kinds of things are broken that need not be. In reality this is totally ignored so best to just delete this sentence. Several places we say unassociated devices can not transmit data frames, which is also wrong. Pretty much most of what we have for use of short addresses is probably wrong (probably was by 2007).

Delete the “shall not” and the rest of the sentence. Note: we should search for “shall not” as most uses will be wrong. We should treat “shall not” as a possible indication of poor specification (try to think “how do we verify this doesn’t happen”).

6.7.1 Transmission

Each time a Data frame or a MAC command is generated,

Probably should be “Each time a Data frame or MAC command frame including the DSN field is generated” though as written it is not wrong, but requires incrementing the DSN even when the field is elided. One might expect the DSN to increment uniformly in frames containing the sequence number field, which would not be the case according to the standard now if some frames elide DSN. There is really no reason to require incrementing the DSN after transmitting a frame without the DSN. This is left over from a simpler time.

Typo: Each device shall generate exactly one dDSN…

First paragraph we have “dDSN” when we mean “DSN”. I thought about adding a definition for dDSN just to be silly (deferred DSN?). We’re silly enough without trying.

The value of macDsn shall be permitted to roll over.

“shall be permitted” is not correct use of normative language. “Permitted” means you may or may not. The word for that is “May” which in this case is wrong. The sequence numbers must roll over. Otherwise it is even less useful as after less than 255 messages the DSN will become constant.

This should be “The value of macDSN shall roll over upon reaching the maximum value representable in the sequence number field” or something like that. Same for BSN.

NOTE—The DSN, BSN, and EBSN are 8-bit values and, therefore, have limited use to the next higher layer (e.g., in the case of the DSN, in detecting retransmitted frames).

This note needs to be stronger IMO as folks still don’t get it. The point is that **using DSN (alone) for duplicate detection is a bad idea**.If not qualitied by source address, worse than useless. Could change “limited” to “no”. Yes, people still do it. And wonder why the miss frames. I’d prefer something like “only an idiot would use the DSN alone for duplicate detection” but that may not meet IEEE-SA guidelines for appropriate language. Maybe I’ll put that on a t shirt.

transmissions in a GTS shall not use CSMA-CA

This is and always has been wrong. But it was easy. The problem is if you use CSMA you have to account for uncertainty in the channel access time when sizing the slots. That’s not a good reason to prohibit what can be useful. We should change this to “may use” or simple delete the statement.

This reflects the invalid assumption that a dedicated timeslot is “contention free” – that is ignoring that there may be users of the band not adhering to our schedule. There is nothing guaranteed about a GTS except that a handful of cooperating devices won’t use it. If DSME is ever used, this is broken for DSME also. We should fix it because it reinforces an incorrect notion that there can be exclusive timeslots, which is rarely the case (The SUN-FSK PHY does support a couple licensed bands which is the only case where there can be anything close to a guarantee). TSCH already allows for CSMA in any slot. Anything added in the future should. So let’s terminate the idea of prohibiting CSMA right now.

6.7.2

The MAC sublayer shall, therefore, be able to filter incoming frames and present only the frames that are of interest to the next higher layer.

Not a valid “shall”. Want to guess why? Ok so no…what is “of interest” ? The MAC has no idea what is of interest to a higher layer. What the MAC knows is if the frame passes the filtering steps.

The correct word is “will” (a statement of fact – the filtering requirements are stated in the following paragraphs).

Note most implementations of promiscuous mode (sniffers) accept frames that fail the FCS. This is useful for sniffers to do. One could argue a sniffer is not a compliant device, but this was the one of the reasons to have promiscuous mode so we should allow that in promiscuous mode all of the filtering may be skipped.

Fourth level flitering, step (e): should have “if source PANID is present”

But we have “If the Source PAN ID field is not included in the frame and the Destination PAN ID field is included in the frame, the MAC sublayer shall use the value of Destination PAN ID field as the source PAN ID” later (should be sooner?). This needs to be before step e) and include the case where neither is present. Should have been changed in 4e or after. Heck it’s only been 11 years!

6.7.4.4 Retransmissions

A device that sends a frame with its AR field set to acknowledgment requested shall wait for the corresponding Ack frame to be received. If an Ack frame is received within the expected time and contains the same DSN as the original transmission, the transmission is considered successful, and no further action regarding retransmission shall be taken by the device.

This is only true when the DSN is present. Need to add “when present”. The DSN is only in the ack if there was a DSN in the frame being acknowledged.

8.2.1 Primitives supported by the MLME-SAP interface

The MLME-SAP allows the transport of management commands between the next higher layer and the MLME. Table 8-1 summarizes the primitives supported by the MLME through the MLME-SAP interface. Primitives marked with a diamond () are optional for an RFD. Primitives marked with an asterisk (\*) are optional for both device types (i.e., RFD and FFD). Primitives marked with a circle () are optional for both RFD-RX and RFD-TX device types.

We have at least 4 device types listed. Delete “for both device types”.

When the optional TSCH mode is implemented (i.e., macTschEnabled = TRUE), the primitives listed in Table 8-2 shall be implemented.

The definition of macTschEnabled is that it indicates that TSCH is **in use**. TSCH may be implemented but inactive in which case macTschEnabled will be FALSE. TSCH may not be implemented in which case macTschEnabled is not implemented. Delete the parenthetical as it is wrong.

In a DSME-enabled PAN, the primitives listed in Table 8-3 shall be implemented.

Similar problem. We mean When DSME is supported, the following primitives are required.

8.4.2 MAC Constants

Table 8-93: aUnitBackoffPeriod isn’t a constant as it may depend on phyCcaDuration. This definition doesn’t really make any sense. I \*think\* it might have once, when there was one PHY, only one symbol duration, etc. I \*think\* the rational for using aTurnaroundTime is that before the first CCA it might be necessary to enable the receiver, that is, switch from transmit to receive. However after the first CCA this would not be necessary. Using the CCA duration doesn’t make sense to me at all. I think this persists because no one has figured out what makes sense (including me).

6.4.1 Association

The next higher layer shall attempt to associate only after having first performed a MAC sublayer reset, by issuing the MLME-RESET.request primitive with the SetDefaultPIB set to TRUE…

Requirements for the next higher layer are out of scope of this standard. Also, most of this is way, way obsolete. Default PIB values are mostly wrong, scan is often not used. And so on. Also “shall attempt” is not a valid statement of requirement. Do or do not as Yoda would say. WRT shall at least, there is no “Try” 😊.

the next higher layers shall request through the MLME-ASSOCIATE.request primitive, …

the next higher layer shall terminate any tracking of the beacon.

Incorrect for the same reason (out of scope). This is a statement of fact or assumption so “will” is the correct word. Possibly “can” if it is possible but not always what happens.

We should search for all occurrences of “the next higher layer [shall|should|may]” because all are wrong and we need to figure out what is really correct. In some cases, e.g. if the order of invoking primitives is essential, we should add behaviors of the MAC for when the order is not followed correctly. In other words, instead of “the higher layer shall” or “the higher layer should” we need “if the higher layer hasn’t first done x then then the MAC will do something” (and ‘fall over in a heap’ might be the best something).

We can state what the MAC \*assumes\* the NHL has done where we can’t really know what to do if it doesn’t. When “assume” appears in a standard it is a red flag that the protocol isn’t well designed – and so if that’s the case we should admit it and move on. Then implementers have a chance.

In other cases it’s just the wrong word (we really mean “can” or “will”). So those are easy.

In a few we have “the next higher layer shall be notified” which is a MAC action (though we could have said it better) and so OK. We got ~~most~~ some of these in the 2015 revision but missed a few. There may be some other places I didn’t find where we are prescribing requirements on the NHL.

Clause 3: The following definitions should be added to clause 3:

Scurry: a collection of squirrels

Dray: a group of squirrels sharing a common nest