**IEEE P802.15**

**Wireless Specialty Networks**

|  |  |
| --- | --- |
| Title: | **Fixing Security Issues in the 4ab draft** |
| Date Submitted: | 2025-10-05 |
| Name: | Tero Kivinen | Affiliation: | Wi-SUN Alliance | E-Mail | kivinen@iki.fi |
| Abstract: | Provide secure format for compact frames, replacing the current broken format in 4ab draft. |

|  |
| --- |
|  **Change history of this document** |
| **Revision** | **Date** | **Description** |
| 15-25-0505-00 | 2025-10-05 | Initial version |
|  |  |  |
|  |  |  |

1. Issues with current secured compact frame formats

The current proposal trying to provide security the compact frames is broken, as the nonce can be trivially be protected, and the format can only be used in the block based mode. The nonce uses Block index as part of the frame counter, and the Block index can be set by the attacker by sending Start of Ranging Compact frame.

The Start of Ranging Compact frame cannot be protected, as the frame counter used to protect it, depends on the starting block index field inside the frame, and also Start of Ranging Compact frame is not part of any ranging block, but is outside of them, making it impossible to be protected.

The attack goes like this:

1. Attacker listens one block ranging operation between devices using encrypted secured compact frames.
2. Attacker sends new Start of Ranging Compact frame that sets the Starting block index back to the same value it had in step 1.
3. Attacker now listens frames from recipient, and as those uses same frame counter than in the previous step, it can simply XOR the encrypted frames with same frame counter to each other and break the encryption of the frame.
4. This causes security vulnerability in the whole system.

If the recipient verifies that starting block index can’t go backwards, i.e., it always needs to be larger than previously seen, then the attacker can cause easy denial of service attack by sending one Start of Ranging Compact frame where the Starting block index is set to 0xffff, and after that recipient will reject all secured frames, and rekey is required to recover from the situation.

1. Protecting compact frames by encapsulating them to standard frames
	1. General

The TG4ab draft contains new frame format called compact frames, which has serious security shortcomings.

* Not all of the frames can be secured
* When secured it requires upper layer coordination to be able to keep frame counters in sync and not to reuse frame counters.
* As the parts of the frame counter is sent inside the unsecured frames this provides ability for attacker to break the security completely

This document provides and alternative way to do same thing but using existing IEEE Std 802.15.4 frame formats.

* 1. Options

In IEEE Std 802.15.4 there is multiple ways to do same things, and depending on the properties required different options can be selected. Here is some possible options:

* MAC Command frames
* Multipurpose frames containing IEs
* Multipurpose frames with version number of 0b01 or 0b10.
	+ Add new version of multipurpose frame which has one octet (version 0b01) or two octet (version 0b10) of sub-id field after the header before IEs.

All above use normal addressing formats, and can use the privacy addresses specified in the TG4ac. Different addressing schemes are used depending on the environment:

* SrcAddrMode of NONE meaning no addresses, when the source frame address is already known (i.e., it is coordinator or whoever is initiating the system), and DstAddrMode of SHORT or EXTENDED with or without PAN ID.
* SrcAddrMode of SHORT or EXTENDED with or without PAN ID and a DstAddrMode of NONE with *macImplicitBroadcast* set to true (i.e., when the message is to be sent to group of devices).

These methods allow 0/2/4/8/10 octet long addressing fields with full privacy if needed.

This document selected the MAC Command frames option.

1. MAC Command frame format
	1. General format

This format uses MAC Command frames to send the compact frames. Each Compact frame type is allocated one MAC Command ID (17 command IDs), and as the addressing fields are already in the MHR PRA Hash and PRA Prand are not needed and are omitted from the compact frames.

The Content field of the MAC command contains the Message ID and Message Content from the Compact Frame.

Frames shall be formatted as illustrated in Figure 1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Octets: 2** | **0/1** | **variable** | **variable** | **variable** | **1** | **1** | **variable** | **2/4** |
| Frame Control | Sequence Number | Addressing fields | Auxiliary Security Header | IE | Command ID | Message ID | Message Content | FCS |
| Header IEs | Payload IEs |
| MHR | MAC Payload | MFR |

1. —MAC Command frames for compact frames
2. Changes to the P802.15.4ab-D03 draft
	1. Clause 7 MAC frame formats changes

Add following entries to table 7-11:

| Command ID | Command name | Subclause |
| --- | --- | --- |
| <ANA> | Compact frame: Advertising Poll | 10.39.11.4, 10.39.11.3.1 |
| <ANA> | Compact frame: Advertising Response | 10.39.11.4, 10.39.11.3.2 |
| <ANA> | Compact frame: Start of Ranging | 10.39.11.4, 10.39.11.3.4 |
| <ANA> | Compact frame: One-to-one Poll | 10.39.11.4, 10.39.11.3.5 |
| <ANA> | Compact frame: One-to-one Response | 10.39.11.4, 10.39.11.3.6 |
| <ANA> | Compact frame: One-to-one Initiator Report | 10.39.11.4, 10.39.11.3.7 |
| <ANA> | Compact frame: One-to-one Responder Report | 10.39.11.4, 10.39.11.3.8 |
| <ANA> | Compact frame: Advertising Confirmation | 10.39.11.4, 10.39.11.3.3 |
| <ANA> | Compact frame: One-to-many Poll | 10.39.11.4, 10.39.11.3.9 |
| <ANA> | Compact frame: One-to-many Response | 10.39.11.4, 10.39.11.3.10 |
| <ANA> | Compact frame: One-to-many Responder Report | 10.39.11.4, 10.39.11.3.11 |
| <ANA> | Compact frame: One-to-many Initiator Report | 10.39.11.4, 10.39.11.3.12 |
| <ANA> | Compact frame: Public Advertising Poll | 10.39.11.4, 10.39.11.3.13 |
| <ANA> | Compact frame: Public Advertising Response | 10.39.11.4, 10.39.11.3.14 |
| <ANA> | Compact frame: Public Start of Ranging | 10.39.11.4, 10.39.11.3.15 |
| <ANA> | Compact frame: Public Advertising Confirmation | 10.39.11.4, 10.39.11.3.16 |
| <ANA> | Compact frame: Acquisition | 10.39.11.4, 10.39.11.3.17 |
| <ANA> | Compact frame: Vendor Specific | 10.39.11.4, 10.39.11.3.18 |

* 1. Clause 8 MAC services changes

Remove CompactSecurityEnabled, and CompactSecurityParams from the Table 1. Remove last sentence of the CompactFrameID Description.

Remove the “The CompactSecurityParams structure groups the parameters specifying Compact frame security. The elements of the CompactSecurityParams are defined in Table 2.” and remove Table 2 from the section 8.3.4.

* 1. Clause 9 Security changes

Remove all changes to the Clause 9. They are not needed, as this secured format uses standard security format.

* 1. Clause 10.32.3.5 Hyper block mode changes

Remove following paragraphs:

If secure Compact frames are used in hyper block mode, the controller shall ensure that the values of hyper block index and relative block index does not cause the value of the ranging block index to exceed 216 – 1.

NOTE—The maximum value of ranging block index in this case is restricted by the size of the Block Index field of the Frame Counter field for Compact frame nonce as specified in 9.3.2.4.

* 1. Clause 10.38 Compact frame format changes

Remove value “17 Secured” from the Table 10.

* 1. Clause 10.39.11 Messages for MMS UWB operation changes

In section 10.39.11.1.1 General remove “, or with a MIC field which shall be one of MIC-32, MIC-64, MIC-128, ENC-MIC-32, ENC-MIC-64 or ENC-MIC-128 as defined by Table 9-6” from the first paragraph.

Remove section 10.39.11.1.2.3 Extended Address completely.

* 1. Clause 10.39.11.2 Security of MMS Compact frames changes

Replace whole section “10.39.11.2 Security of MMS Compact frames” with following paragraph:

Any secured compact frame may be secured by using the MAC Command frames as described in 10.39.11.4. Those MAC Command frames uses standard addressing fields, thus they may use normal security described in Clause 9.

Remove tables 25 and 26.

* 1. Clause 10.39.11.3.19 removal

Remove clause 10.39.11.3.19 Secured Compact frame, as that is no longer needed as this secured format uses standard security format.

* 1. Clause 10.39.11.4 addition

Add new section 10.39.11.4 MAC Command format for compact frames as follows:

Each compact frame is allocated an Command ID that can be used to embed the compact frame inside the MAC Command frame format. This allows using standard security, privacy and other features provided by standard frames.

Frames shall be formatted as illustrated in Figure 2.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Octets: 2** | **0/1** | **variable** | **variable** | **variable** | **1** | **1** | **variable** | **2/4** |
| Frame Control | Sequence Number | Addressing fields | Auxiliary Security Header | IE | Command ID | Message ID | Message Content | FCS |
| Header IEs | Payload IEs |
| MHR | MAC Payload | MFR |

1. —MAC Command frames for compact frames

The Command ID for each compact frame type is specified in Table 7-11. Message ID is described in section 10.39.11.1.3.1. The Message Contents field contains the Message Content field of the compact frame.