IEEE P802.11
Wireless LANs

|  |
| --- |
| BSS Privacy – Frame Anonymization  |
| Date: 2024-09-06 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jerome Henry | Cisco Systems |  |  | jerhenry@cisco.com |
| Domenico Ficara | Cisco Systems |  |  | dficara@cisco.com |
| Ugo Campiglio | Cisco Systems |  |  | ucampigl@cisco.com |
| Javier Contreras | Cisco Systems |  |  | jacontre@cisco.com |
| Jarkko Kneckt | Apple Inc. |  |  | jkneckt@apple.com |

Abstract

This submission solves the CIDs 1521 of the 802.11bi internal comment collection.

The submission defines BSS Privacy (BP) operations to meet the 802.11bi requirements [1] 18, 39 and 40.

This submission builds on top of the 802.11bi Draft 0.4.

[1] 11-21-1848-16-00bi-requirements-document

|  |  |  |  |
| --- | --- | --- | --- |
| **CID** | **Comment** | **Proposed Change**  | **Proposed Resolution** |
| 1521 | 802.11bi defines requirements for the BSS Privacy Enhancements (BPE). Please add procedures needed for BPE anonymizations. | Please define BPE procedures that use encrypted Beacon as in 22/1306, allow AP discovery only for preconfigured STAs, anonymize STA and AP addresses and anonymization of the multicast transmissions. | Revised. Agree in principle. Please include the submission 11-24-1579r0 on BSS Privacy Beaconing and this submission on BP anonymization to the 802.11bi draft. |

### This normative text meets the following 802.11bi requirements: [1]

|  |  |  |
| --- | --- | --- |
| **Requirement ID** | **Requirement**  | **Status** |
| 18 | 11bi shall define a mechanism for a BPE AP to facilitate changing its AP identification information while there are Clients associated, without disrupting the connectivity from the Clients, and/or clients in the process of associating. | **Approved** (Motion #17, July 13, 2022) |
| 39 | 11bi shall define a mechanism for a BPE AP and a BPE Client to change the OTA MAC addresses, SN and PN they use for unicast transmissions. | **Approved** (Motion #20, 14 Sept 2022) |
| 40 | 11bi shall define a mechanism for a BPE AP to obfuscate the RA, SN and PN of the group frames to avoid BPE AP tracking. | **Approved** (Motion #20, 14 Sept 2022) |

**Normative text:**

*TGbi editor: Add the following text at the end of the clause 10.71.8*

10.71.8 BSS Privacy Operations

The associated non-AP BP MLDs and BP AP MLD operate in a single EDP group named as BP group. The BP group has a single schedule. At the beginning of each epoch, the BP non-AP STA addresses and SN spaces and PNs of the individual frames are anonymized in all links according to CPE anonymization, see10.71.1.3(Establishing frame anonymization parameter sets). The BP AP addresses, the Timestamp field of the Privacy Beacons and the group frames are anonymized according to BPE anonymization, see 10.71.1.4(Establishing BP frame anonymization parameter sets).

*TGbi editor: Add the following new clause 10.71.8.2*

10.71.8.2 Group addressed frames anonymization

A BP AP shall anonymize group addressed frames by using the offsets as described in 10.71.3.4(Establishing BP frame anonymization parameter sets):

* The MAC header anonymization parameters are selected as described in 10.71.4.1(MAC header anonymization).
* The OTA group address is anonymized as described in 10.71.4.4(Addressing).
* The SN is anonymized with the SNS1 DL offset as described in 10.71.4.2.(Sequence number anonymization).
* The PN is anonymized with the PN Group offset as described in 10.71.4.3(Packet number anonymization).

A BP STA shall de-anonymize the received group frames by using the offsets as described in 10.71.3.4(Establishing BP frame anonymization parameter sets):

* The transmitter address is filtered as descried in 10.71.5.1(Address Filtering).
* The group address is deanonymized as described in 10.71.4.4(Addressing).
* The PN is deanonymized with the PN Group offset as described in 10.71.5.3(Packet number anonymization).
* The SN is deanonymized with the SNS1 DL offset as described in 10.71.5.4(Sequence number anonymization).

To improve the BP AP privacy, the BP AP shall use GTK to encrypt the payload of the group management frames.

*TGbi editor: Add the new field to the Enhanced Data Privacy element*

**9.4.2.337 Enhanced Data Privacy (EDP) element**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Reserved | Reserved | Epoch Interval Duration | Next Epoch Start Time | Time Range | Reserved | EpochSequenceDuration | BP Epoch Number |
| Bits: | 11 | 11 | 14 | 64 | 16 | 4 | 8 | 48 |

The BP Epoch Number in an unsigned integer that is increased by one for each BP epoch.

*TGbi editor: Apply the following changes to 10.71.3 (Establishing frame anonymization parameter sets).*

10.7.1.3 Establishing frame anonymization parameter sets

This subclause describes how an AP MLD and associated non-AP MLD establish the CPE FA parameter set for each EDP epoch for the CPE non-AP MLD. The BP FA parameter sets creation is described in 10.7.1.4 (Establishing BP frame anonymization parameter sets).

The non-AP MLD and AP MLD establish(#Ed) the EDP epochs used for frame anonymization as described in 10.71.2 (EDP epoch operation).

*TGbi editor: Add the new clause 10.71.1.4.*

**10.71.1.4 Establishing BP frame anonymization parameter sets**

All associated BP non-AP MLDs and the BP AP MLD shall generate EDP BP frame anonymization parameters for a given EDP epoch by computing a single pseudorandom EDP BP FA block which is partitioned into the set of EDP BP frame anonymization parameters according to the Table 10-XX (EDP BP FA block bit positions).

For a given EDP epoch, the EDP FA block shall be generated as:

EDP\_BP\_FA\_block = KDF-Hash-Length (BPDK, “EDP BP frame anonymization”, BP Epoch Number)

, where:

KDF-Hash-Length is the key derivation function as defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-190 (AKM suite selectors)); Length is equal to 872 bits for offset calculation.

BPDK is the BSS Privacy Derivation Key.

BP Epoch Number is the BP Epoch Number to which the offset is calculated (see 9.4.2.337 (Enhanced Data Privacy (EDP) element)).

The BP offsets for the Group PN, SNS1 DL, SNS11 DL and Timestamp together with the anonymized BP AP link addresses are created from the EDP\_BP\_FA\_block. The offsets and the AP link addresses have static assignments to the EDP\_BP\_FA\_block as shown in the Figure 10-XX (EDP BP FA block bit positions).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| BP offsets and AP addresses | Group PN Offset | SNS1 DL Offset | SNS11 DL Offset | Timestamp Offset | Group Anonymization Key | Anonymized AP Link Addresses  |
| Assigned random bits | 0 – 47 | 48 –59 | 60 –71 | 72 - 135 | 136 – 181 | 182 – 871 |
| Size (bits) | 48 | 12 | 12 | 64 | 46 | 690 |

**Table 10-XX EDP BP FA block bit positions**

The 46 bits of the Group Anonymization Key anonymizes the group addresses as described in 10.71.4.4(Addressing). All bits of the group address are anonymized, except the Group/Individual bit shall be set to 1 and the Local/Global bit value shall not be modified.

The 46 bits of the AP link addresses are anonymized. All bits of the AP link address are anonymized, except the Group/Individual bit shall be set to 0 and the Local/Global bit shall be set to 0.

Table 10-xx EDP BP FA block bit positions of BP AP link addresses

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Link ID | Bit positions | Link ID | Bit positions | Link ID | Bit positions |
| 0 | 182:227 | 5 | 412:457 | 10 | 642:687 |
| 1 | 228:273 | 6 | 458:503 | 11 | 688:733 |
| 2 | 274:319 | 7 | 504:549 | 12 | 734:779 |
| 3 | 320:365 | 8 | 550:595 | 13 | 780:825 |
| 4 | 366:411 | 9 | 596:641 | 14 | 826:871 |

*TGbi editor: Add the new paragraph at the end of the clause 10.71.4.2.*

* Sequence number anonymization

If the MAC header of the frame includes a Sequence Control field using DL sequence number space SNS1 (Baseline) or sequence number space SNS11 (Group addressed data) (see Table 10-5 (Transmitter sequence number spaces)), then the transmitter shall compute an over-the-air SN (OSN) value from the sequence number SN assigned to the MPDU as follows:

 OSN = (SN + EDP\_SN\_offset) mod 212,

where EDP\_SN\_offset is the SNS specific offset value, generated as specified in 10.71.4 (Establishing BP frame anonymization parameter sets).

*TGbi editor: Modify the clause 10.71.4.4 as shown below*

* Addressing

MLD addressing shall be applied per 35.3.2 (MLD addressing) with the following addressing clarification:

* The MAC address of a STA affiliated with a non-AP MLD corresponding to a link is the EDP\_STA\_MAC value assigned to that link in the selected MAC header anonymization parameter set.
* If a STA of BP MLD transmits a frame, the address of the AP affiliated with BP AP MLD is the EDP\_AP\_MAC value assigned to the link in the **EDP BP frame anonymization set**.
* If a STA of BP MLD transmits a group frame, the group address of the frame is anonymized as follows:

OGroupAddress = (group address + EDP Group Anonymization Key) mod 246,

where group address is 46 bits of the address excluding the local/global and individual/group bits.

EDP Group Anonymization Key is specified in 10.71.4 (Establishing BP frame anonymization parameter sets).

* If a STA of BP MLD receives a group frame, the group address of the frame is deanonymized as follows:

Group address = OGroupAddress - EDP Group Anonymization Key) mod 246,

where OGroupAddress is 46 bits of the received group address excluding the local/global and individual/group bits.

EDP Group Anonymization Key is specified in 10.71.4 (Establishing BP frame anonymization parameter sets).

*TGbi editor: Add the following text as the second and third paragraph of the clause 10.71.5.1*

* Address filtering

During the transition period (see 10.71.2.1 (Introduction) and 10.71.2.5 (Epoch boundaries)) from an old EDP epoch to a new EDP epoch of the BP non-AP MLD, the affiliated STA of the BP non-AP MLD and the affiliated AP of the BP AP MLD (on a setup link of the BP non-AP MLD) shall perform address filtering using:

* the EDP\_STA\_MAC and anonymized AP address from the MAC header anonymization parameters (if any) of the old EDP epoch,
* the anonymized AP address and anonymized group address from the MAC header anonymization parameters (if any) of the old EDP epoch,
* the EDP\_STA\_MAC and anonymized AP address from the MAC header anonymization parameters (if any) of the new EDP epoch,
* and the anonymized AP address and anonymized group address from the MAC header anonymization parameters (if any) of the new EDP epoch.

After this transition period, until the start of the transition period of the next EDP epoch of the BP group, the affiliated STA of the BP non-AP MLD and the affiliated AP of the BP AP MLD (on a setup link of the BP non-AP MLD) shall perform address filtering using:

* the EDP\_STA\_MAC and AP anonymized address from the MAC header anonymization parameters of the new EDP epoch,
* and the anonymized AP address and anonymized group address from the MAC header anonymization parameters (if any) of the new EDP epoch.

*TGbi editor: Add the following text at the end of the clause 10.71.5.4*

* Sequence number deanonymization

For frames using DL sequence number space SNS1 (Baseline) or sequence number space SNS11 (Group addressed data) (see Table 10-5 (Transmitter sequence number spaces)), the receiver shall compute the original SN value from the value in the sequence number field, OSN, as follows:

SN = (OSN − EDP\_SN\_offset) mod 212,

where EDP\_SN\_offset is the SNS specific offset value, generated as specified in 10.71.4 (Establishing BP frame anonymization parameter sets).